НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ імені ІГОРЯ СІКОРСЬКОГО»

Інститут телекомунікаційних систем

Кафедра Інформаційно-телекомунікаційних мереж

До захисту допущено:

Завідувач кафедри

_____ Лариса ГЛОБА

«___»_____2020 р.

Дипломна робота

на здобуття ступеня бакалавра

за освітньо-професійною програмою «Інформаційно-комунікаційні технології»

спеціальності 172 «Телекомунікації та радіотехніка»

на тему: «Аналіз застосування IoT для дослідження трафіку на автошляхах»

Виконала:
студентка IV курсу, групи ТІ- 62
Власенко Тетяна Ігорівна _____

Керівник:
доцент кафедри ІТМ ІТС, доцент, к.т.н.
Правило Валерій Володимирович _____

Рецензент:
доцент кафедри ТК ІТС, доцент, к.т.н.
Явіся Валерій Сергійович _____

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Студентка _____

Київ – 2020 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Інститут телекомунікаційних систем

Кафедра Інформаційно-телекомунікаційних мереж

Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 172 «Телекомунікації та радіотехніка»

Освітньо-професійна програма «Інформаційно-комунікаційні технології»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ Лариса ГЛОБА

«___»_____2020 р.

ЗАВДАННЯ

на дипломну роботу студентці

Власенко Тетяні Ігорівні

1. Тема роботи «**Аналіз застосування IoT для дослідження трафіку на автошляхах**», керівник роботи доцент кафедри інформаційно-телекомунікаційних мереж ІТС Правило Валерій Володимирович, доцент к.т.н., затверджені наказом по університету від «30» березня 2020 р. № 924-с.

2. Термін подання студентом роботи 8 червня 2020 р.

3. Вихідні дані до роботи: 1.Спеціальна література

2.Матеріали мережі інтернет.

3. Вибрана платформа аналізу трафіку на автошляхах для удосконалення.

4. Зміст роботи:

1) Розглянути основні аспекти роботи мережі IoT, їх класифікація та

призначення, принципи їх побудови, необхідні умови для повноцінного функціонування мережі, переваги та недоліки.

2) Провести аналіз існуючих систем моніторингу трафіку на автошляхах та на основі даних систем провести порівняльний аналіз ефективності застосування, виділити переваги і недоліки аналізу трафіку.

3) Представити вдосконалену систему IoT для дослідження та контролю трафіку на автошляхах.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо)

Презентація по темі “ Аналіз застосування IoT для дослідження трафіку на автошляхах ” в кількості 11 слайдів

Слайд №1 – Тема роботи;

Слайд №2 – Актуальність роботи;

Слайд №3 – Мета роботи;

Слайд №4 – Задачі, які виконуються в роботі;

Слайд №5 – Розділи;

Слайд №6 - Аспекти роботи мережі IoT;

Слайд №7 - Платформи моніторингу трафіку;

Слайд №8, 9 – Практична частина;

Слайд №10 – Висновки по роботі;

Слайд №11- Публікації

6. Дата видачі завдання 10 вересня 2019 р.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1.	Вступ	21.11.2019	виконано
2.	Розглянути основні аспекти роботи мережі IoT	11.03.2020	виконано
3.	Провести аналіз існуючих систем моніторингу трафіку на автошляхах	8.04.2020	виконано

4.	Провести порівняльний аналіз ефективності застосування існуючих систем, виділити переваги і недоліки аналізу трафіку	26.04.2020	виконано
5.	Представити вдосконалену систему IoT для дослідження та контролю трафіку на автошляхах	20.05.2020	виконано
6.	Висновки	25.05.2020	виконано

Студентка Тетяна ВЛАСЕНКО

Керівник роботи Валерій ПРАВИЛО

РЕФЕРАТ

Робота містить 72 сторінки та 17 рисунків. Було використано 19 джерел.

Метою роботи є аналіз застосувань IoT та нових підходів моніторингу для дослідження трафіку на автошляхах.

Об'єктом дослідження є вдосконалення способів моніторингу трафіку на автошлях із застосуванням IoT.

Предметом дослідження є технології IoT для дослідження трафіку на автошляхах.

В даній роботі розглядаються основні аспекти роботи мережі IoT , їх класифікація та призначення, принципи їх побудови, необхідні умови для повноцінного функціонування мережі. Досліджено архітектуру та основні компоненти IoT. Розглянуто еталону модель, безпеку і захисти безпеки IoT. - Наведено переваги та недоліки, які притаманні мережам IoT. Визначення моніторингу та аналіз платформ моніторингу, які впливають на ефективність роботи різних платформ. Для досягнення поставленої мети було проведено визначення існуючих систем моніторингу трафіку на автошляхах та аналіз основних недоліків систем; оцінка і порівняльний аналіз платформ OnStar, NEXCO Central, ECall Japan, ECall Europe. Також розглянуто такі системи як: система аналізу дорожнього руху (RTA), Моха та система моніторингу дорожнього руху в режимі реального часу з використанням алгоритму SAR**.** Запропонована вдосконалена система для контролю трафіку цілодобово з урахуванням всіх недоліків проаналізованих систем аналізу дорожнього руху.

Отримані результати дозволять ефективно аналізувати стан на дорогах та трафік на автошляхах, що призведе до зменшення кількості завантаженості на автошляхах, аварій та економії часу.

Ключові слова: Інтернет речей, трафік, транспортні засоби, датчики, сервер.

ABSTRACT

The work contains 72 pages and 17 figures. 19 sources have been used.

Goal: research an analysis of applications of IoT and new approaches of monitoring is for research of traffic on motorways.

A research object is perfection of methods of monitoring of traffic on a motorway with application of IoT.

In this work the basic aspects of work of network of IoT, are examined their classification and setting, principles of their construction, necessary terms for the valuable functioning of network. Architecture and basic components of IoT are investigational. A model is considered to the standard, safety and protect safety of IoT. Advantages over and defects are brought, what inherent to the networks of IoT. Determination of monitoring and analysis of monitoring platforms that influence on efficiency of work of different platforms. For the achievement of the put aim determination of the existent systems of monitoring of traffic on motorways and analysis of basic lacks of the systems was conducted; estimation and comparative analysis of platforms OnStar, NEXCO Central, ECall Japan, ECall Europe. Such systems are also considered as: system of analysis of travelling motion (RTA), Moxa and system of monitoring of travelling motion real-time with the use of algorithm of SAR. Offer improved system for control of traffic around the clock taking into account all lacks of the analysed systems of analysis of travelling motion.

The article of research are technologies of IoT for research of traffic on motorways.

The obtained results will allow to effectively analysing the state on roads and traffic that will result in reduction to the amount of workload on motorways, accidents and economy of time.

Key words: IoT, traffic, transport vehicles, sensors, server.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

IoT	Internet of Things
GPS	Global Position System
DAS	Digital and Analog Systems
WAN	Wide Area Network
MQTT	MQ Telemetry Transport
LWM2M	Lightweight Machine - to – Machine
CoAP	Constrained Application Protocol
JSON	JavaScript Object Not
WLAN	Wireless Local Area Network
RTOS	Real-Time Operating System
M2M	Machine-to-Machine
IDS	Intrusion Detection System
NMS	Network Monitoring System
SLA	Service Level Agreement
SAR	Specific Absorption Rate
GMTI	Системи і алгоритми, створені у військовій області
RTA	Система аналізу дорожнього руху
FFT	Fast Fourier transform
SNR	Signal-to-Noise Ratio
IEEE	Institute of Electrical and Electronics Engineers
WLAN	Wireless Local Area Network
RSU	Road Side Unit
LCD	Liquid Crystal Display

ВСТУП

IoT - це нова парадигма, яка швидко набирає оберти в сценарії безпровідного зв'язку. Це новітня технологія, що має унікальну ідентифікацію і дозволяє об'єктам взаємодіяти один з одним для отримання даних на веб-сервері, для зберігання і збору даних і для спільної роботи з користувачами. Таке розумне спілкування дає IoT без людської взаємодії.

У зв'язку з урбанізацією числа доріг, транспортні засоби нестримно ростуть. Моніторинг руху і контроль за ним кидають виклик багатьом містам нашої країни. Більшість міст досі страждають від пробок і пов'язаних з ними проблем. У зв'язку з цим виникає безліч проблем, таких, як затримка в русі між двома великими містами, витрата палива на перехрестях, забруднення повітря із-за викидів, загибель людей на дорогах в результаті аварій і багато проблем, пов'язаних з транспортом. Транспортні засоби, системи датчиків на дорогах і допоміжні системи дорожньої інфраструктури збирають повсякденну інформацію про умови дорожнього руху. Окрім систем датчиків на дорогах, нові транспортні засоби оснащені декількома системами датчиків допомоги водієві. Інформація про датчики для водія з середовища руху обмежена датчиками автомобілів, хоча нові мобільні телефони і навігатори здатні отримувати інформацію в режимі реального часу.Таким чином, можна сказати, що найбільш ефективним рішенням буде інтеграція розглянутих систем в одній універсальній. Це дозволить забезпечити автомобіліста повним спектром послуг, починаючи від ефективної навігації

Мета даної дипломної роботи полягає в аналізі застосувань IoT та нових підходів моніторингу для дослідження трафіку на автошляхах.

Об’єктом дослідження є вдосконалення способів моніторингу трафіку на автошлях із застосуванням IoT.

Предметом дослідження є технології IoT для дослідження трафіку на автошляхах.

РОЗДІЛ 1
ОСНОВНІ АСПЕКТИ РОБОТИ МЕРЕЖІ IoT

1.1 Базові визначення в мережі IoT

Інтернет речей (англ. Internet of Things, IoT) - концепція обчислювальної мережі фізичних предметів («речей»), оснащених вбудованими технологіями для взаємодії один з одним або з зовнішнім середовищем, яка розглядає організацію таких мереж як явище, здатне перебудувати економічні та суспільні процеси, що виключає з частини дій і операцій необхідність участі людини.

Інтернет речей (IoT) відноситься до величезної кількості "речей", які підключені до Інтернету, щоб вони могли обмінюватися даними з іншими речами - IoT-додатками, підключеними пристроями, промисловими машинами і багато що інше. Підключені до Інтернету пристрої використовують вбудовані датчики для збору даних і в деяких випадках діють на них. Підключені до Інтернету речей пристрою і машини можуть поліпшити нашу роботу і життя. Приклади реального Інтернету речей варіюються від розумного будинку, який автоматично регулює опалювання і освітлення, до розумної фабрики, яка стежить за промисловими машинами, щоб шукати проблеми, а потім автоматично настроюється, щоб уникнути збоїв.[5]

Передбачається, що в майбутньому Інтернет-речі стануть активними учасниками бізнесу, інформаційних і соціальних процесів, де зможуть взаємодіяти між собою, обмінюючись інформацією про навколишнє середовище, не потребуючи при цьому втручання людини. Завдяки процесорам і бездротовим мережам в частину IoT можна перетворити все що завгодно – від пігулки до літака. Це додає рівень цифрового інтелекту пристроям, які в іншому випадку були б неактивними, дозволяючи їм спілкуватися без участі людини і поєднання цифрових і фізичних світів. [1]

1.2 Архітектура IoT

Спочатку термін "інтернет речей" був придуманий MIT Auto – ID. Центр в якому з 2001 р. відноситься до архітектури, яка включає чотири елементи:

— рівень датчиків;

— мережевий рівень;

— рівень обробки даних;

— прикладний рівень;

Рівні архітектури Інтернету речей розрізняються для відстежування узгодженості системи. Це також слід враховувати до початку процесу створення архітектури IoT (рис. 1.1)

В основному, існує три рівні архітектури Інтернету речей:

а) Клієнтська сторона (рівень облаштувань Інтернету речей);

б) Оператори на стороні сервера (рівень витягання IoT);

в) Шлях для підключення клієнтів і операторів (рівень платформи IoT;

Крім того, основні функції стійкої архітектури Інтернету речей включають функціональність, масштабованість, доступність і ремонтопридатність. Без урахування цих умов результатом архітектури Інтернету речей є збій. [2]

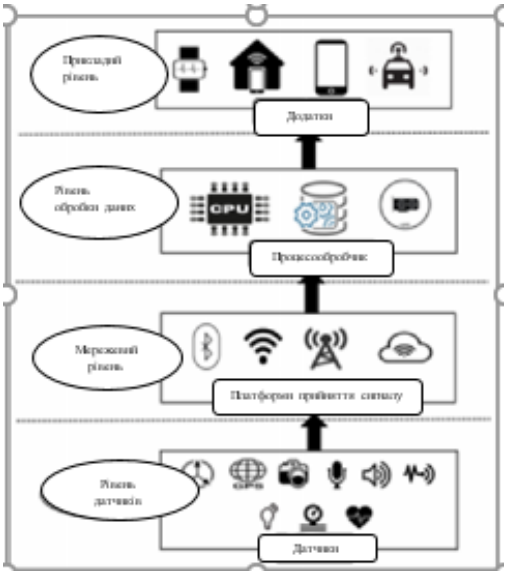

Рис. 1.1 Архітектура мережі IoT

Рівень датчиків

На даному рівні датчики збирають дані з середовища або об'єкту виміру і перетворюють їх на корисні дані. Виконавчі механізми також можуть втручатися для зміни фізичних умов, які генерують дані. Виконавчий механізм може, наприклад, відключати джерело живлення, регулювати клапан повітряного потоку або переміщати автоматизований захват в процесі збору.

Сенсорний етап охоплює все: від традиційних промислових пристроїв до автоматизованих камер, датчиків рівня води, датчиків якості повітря, пульсометрів і моніторів частоти сердечних скорочень. Сфера застосування Інтернету речей швидко розширюється завдяки, зокрема, малопотужним технологіям безпровідної сенсорної мережі і технології Power over Ethernet, які дозволяють пристроям в дротяній локальній мережі працювати без використання джерела живлення A/C.

У архітектурі Інтернету речей деяка обробка даних може відбуватися на кожному з чотирьох етапів. Проте тоді як ви можете обробляти дані на датчику, те, що ви можете зробити, обмежується обчислювальною потужністю, доступною на кожному облаштуванні Інтернету речей. Дані лежать в основі архітектури Інтернету речей, і при обробці цих даних необхідно вибирати між оперативністю і глибиною розуміння. Чим швидше потреба в інформації, тим ближче до кінцевих пристроїв має бути ваша обробка.

Для отримання детальнішої інформації, що вимагає більшої обробки, необхідно перенести дані в хмарну систему або систему центру обробки даних, яка може об'єднати декілька джерел даних. Але деяких рішень просто не може чекати глибока обробка і ви повинні обробити дані прямо на датчику - на самому краю крайової мережі - для найбільш швидкого відгуку.

Датчики в IoT пристроях можуть бути класифіковані на 3 широкі категорії:

— Датчики руху, які вимірюють зміни в русі, а також орієнтацію пристроїв. Є два типи рухів, які можна спостерігати за допомогою датчику цього пристрою: лінійний та кутовий рух. Лінійний рух відноситься до лінійного переміщення пристрою IoT, в той час як кутовий рух відноситься до обертального переміщення пристрою;

— Датчики навколишнього середовища до них відносяться такі пристрої, як датчики світла, датчики тиску та інші, які вбудовані в IoT пристрої реагують на зміни в параметрах навколишнього середовища за допомогою периферійних пристроїв. Основною метою використання цих датчиків в IoT пристроях є допомога пристроям приймати автономні рішення відповідно до змін в периферійних пристроях. Наприклад, датчики навколишнього середовища використовуються в більшості додатків для спрощення життя користувачів (розумні замки, система домашньої автоматизації, розумне освітлення та ін.). Датчики місцеперебування пристроїв IoT взаємодіють з фізичним місцеперебуванням та розташуванням самого пристрою. Найбільш поширеними датчиками місцеперебування, що використовуються в IoT є магнітні датчики та Global Position System (GPS) датчики. Магнітні датчики використовуються, як цифрові компаси та допомагають фіксувати орієнтацію дисплею пристрою. GPS датчики використовується для навігаційних цілей в IoT пристроях.

Мережевий рівень

Головна ціль мережевого рівня – це передача даних від датчиків в аналоговому виді. Ці дані необхідно агрегувати і перетворювати в цифрові потоки для подальшої обробки в низхідному напрямі. Ці функції агрегації і перетворення даних виконуються системами збору даних (DAS). DAS підключається до мережі датчиків, агрегує виходи і виконує аналого-цифрове перетворення. Шлюз Інтернету приймає агреговані і оцифровані дані і направляє їх по Wi - Fi, дротяним локальним мережам або Інтернету в системи етапу 3 для подальшої обробки.

Життєво важливе значення цього рівня полягає в обробці величезного об'єму інформації, зібраної на попередньому етапі, і її стисканні до оптимального розміру для подальшого аналізу. Крім того, тут відбувається необхідна конверсія з точки зору термінів і структури.

Рівень обробки даних

Рівень обробки даних підготовлює дані, які передаються в IT- світ. Зокрема, крайові IT-системи виконують тут розширену аналітику і попередню обробку. Наприклад, йдеться про технології машинного навчання і візуалізації. При цьому тут може статися деяка додаткова обробка, до етапу входу в центр обробки даних.

Оскільки дані Інтернету речей можуть легко збільшити пропускну спроможність мережі і загальмувати ресурси центру обробки даних, краще всього мати системи на краях, здатні виконувати аналітику, щоб понизити навантаження на базову IT-інфраструктуру. Якби у вас був тільки один великий канал для передачі даних в центр обробки даних, вам знадобилася б величезна місткість. Ви також зіткнетеся з проблемами безпеки, з проблемами зберігання і із затримками в обробці даних. Поетапний підхід дозволяє виконувати попередню обробку даних, генерувати значимі результати і їх передавати.

Прикладний рівень

Прикладний рівень вимагає глибшої обробки, яка спрямовуються у фізичні центри обробки даних або хмарні системи, де потужніші IT-системи можуть аналізувати, управляти і безпечно зберігати дані. Для отримання результатів вимагається більше часу, поки дані не досягнуть етапу 4, але можна виконати глибший аналіз, а також об'єднати дані датчиків з даними з інших джерел для отримання детальнішої інформації. Обробка в 4 етапи може відбуватися локально, в хмарі або в гібридній хмарній системі, але тип обробки, що виконується на цьому етапі, залишається тим самим, незалежно від платформи.

1.3 Принцип роботи IoT

Облаштування Інтернету речей містять датчики і міні-комп'ютерні процесори, які впливають на дані, зібрані датчиками, за допомогою машинного навчання. IoT- пристрою є міні-комп'ютерами, підключені до Інтернету і уразливі для шкідливих програм і злому. (рис. 1.2) Машинне навчання - це коли комп'ютери вчаться по аналогії з людьми - збираючи дані зі свого оточення - і це те, що робить IoT- пристрої розумними. Ці дані можуть допомогти машині упізнати ваші переваги і відповідним чином відрегулювати себе. [1] Машинне навчання - виду штучного інтелекту, який допомагає комп'ютерам вчитися без необхідності програмувати. (рис. 1.3)

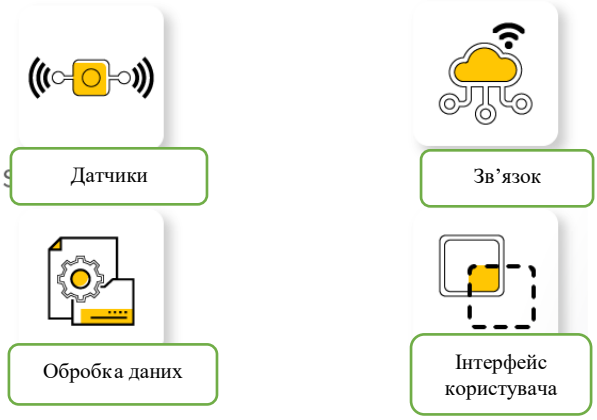

Рис. 1.2 Принцип роботи IoT об'єднує чотири основних етапи:

— Зчитування інформації за допомогою датчиків;

— Передача даних від датчиків до хмарних сховищ;

— Обробка даних отриманих за допомогою датчиків;

— Передача інформації на інтерфейс користувача;

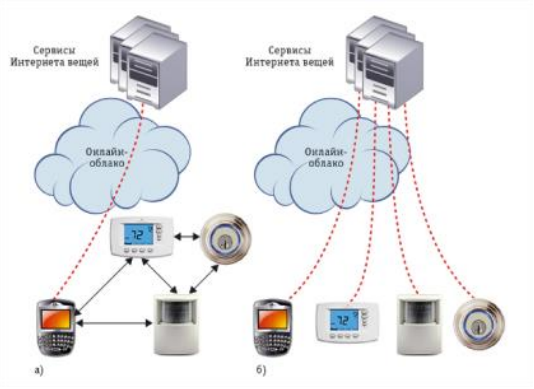

Рис. 1.3 Принцип роботи IoT

Зчитування інформації за допомогою датчиків

Основним компонентом технології Інтернету речей є датчик/пристрій. Датчик витягає усі деталі з довкілля. Довкілля може мати багато складнощів. Що робить безпеку Інтернету речей настільки прекрасною, так це датчики, які підхоплюють навіть найвідчутніші зміни. Ці датчики вбудовані в пристрої, які збирають усі дані для подальшого використання. [4]

Використовується на даному етапі також й пристрої, оскільки декілька датчиків можуть бути об'єднані разом або датчики можуть бути частиною пристрою, що робить більше, ніж просто аналіз даних. Наприклад, ваш телефон - це пристрій з кількома датчиками (камера, акселерометр, GPS тощо), але телефон неє лише датчиком.

Передача даних від датчиків до хмарних сховищ

Після збору даних вони передаються в хмарну інфраструктуру (відому також як платформи Інтернету речей). Але для передачі даних пристроям знадобиться носій, як Bluetooth, Wi - Fi, WAN, стільникові мережі і так далі. Усі ці середовища відрізняються один від одного і мають бути підібрані розумно для досягнення найкращих результатів. Ефективність безпеки Інтернету речей значною мірою залежить від швидкості і доступності цих середовищ.

Обробка даних отриманих за допомогою датчиків

Аналіз проходить дуже просто, як перевірка температури змінного струму або складним. Додаток для Інтернету речей створений таким чином, що воно може швидко обробляти усі дані для вжиття негайних заходів.

Передача інформації на інтерфейс користувача

Користувач отримує повідомлення про дію за допомогою повідомлення або звукового попередження, відправленого мобільним додаткам IoT. Таким чином користувач дізнається, що його команда була виконана через системи.

1.4 Еталонна модель IoT

Модель складається з чотирьох основних рівнів, а також з двох додаткових рівнів: можливості управління та безпеки. [3]

До основних рівнів належить:

- прикладний рівень;
- рівень підтримки послуг та додатків;
- мережевий рівень;
- рівень пристроїв.

1.5 Варіанти архітектури програмного забезпечення

Системи Інтернету речей включають різні драйвери і компроміси. До важливих чинників відносяться витрати, можливості оновлення, можливість динамічного програмування, безпека, енергоефективність і затримка передачі даних. Ці чинники значною мірою визначають описувані нижче варіанти архітектури. На високому рівні варіанти архітектури програмного забезпечення для клієнтських облаштувань Інтернету речей підрозділяються на наступні сім категорій: від простих до складніших:

— архітектура без OS;

— архітектура RTOS (ОС реального часу);

— архітектура під час виконання мовою;

— архітектура повного OS;

— архітектура OS додатка;

— архітектура СЕРВЕР-ОС;

— архітектура контейнерного OS.

Архітектура без OS

Переважна більшість сучасних проблем Інтернету речей дійсно проста. Інтелектуальні лампочки, термостати, дистанційно керовані вилки електроживлення, датчики якості повітря і ідентифікаційні мітки або значки не вимагають складних пакетів програмного забезпечення. Такі прості пристрої для Інтернету речей непотребують ОС або платформи додатків. Усе програмне забезпечення написане спеціально для пристрою, а розробка програмного забезпечення, як правило, здійснюється власними силами. Так що підтримка сторонніх розробників не потрібна. Підтримка оновлень ПЗ може бути обмежена або бути відсутнім. Враховуючи фіксований характер програмного забезпечення в таких облаштуваннях низького рівня, об'єм ОЗУ і флэш-пам’яті може бути зведений до мінімуму. У багатьох випадках досить всього декількох кілобайт або десятків кілобайт оперативної пам'яті. Для облаштувань низького рівня, працюючих від батарей, велику роль грає оптимізація мережевого зв'язку. Важливе значення мають протоколи обміну даними, такі як MQTT (MQ Telemetry Transport), LWM2M (Lightweight Machine - to - Machine) і CoAP (Constrained Application Protocol), тоді як здібніші пристрої, як правило, використовують HTTP- зв'язок і детальніші формати даних, такі як JSON (JavaScript Object Not) або XML.

Архітектура RTOS

Для трохи здібніших пристроїв, що підтримують багатіший набір датчиків, RTOS може бути корисним. Популярні RSTO з відкритим початковим кодом і комерційні RSTO надають зручний набір інструментів для розробників і базовий набір API, що підтримують розробку програмного

забезпечення для інших виробників. Вони також підтримують такі функції продукту, як оновлення вбудованого ПО. Розробка програмного забезпечення для облаштувань Інтернету речей на основі RTOS - зазвичай здійснюється власними силами, оскільки такі пристрої, як правило, не забезпечують загальнодоступні API- інтерфейси сторонніх розробників або можливість динамічно перепрограмувати пристрій (окрім формування повного оновлення вбудованого ПО).

Типовими мовами розробки для пристроїв на основі RTOS являються C або C11, хоча в деяких областях може використовуватися навіть код складання. Вимоги до пам'яті архітектури, грунтованої на RTOS, сумісні з архітектурою без ОС і часто вимагають усього лише декількох десятків кілобайт оперативної пам'яті і декількох сотень кілобайт флэш-памяти. Облаштування цієї категорії часто працюють від батарей, таким чином пред'являючи безліч вимог до оптимізації мережевих з'єднань і споживання енергії в ширшому сенсі.

Архітектура під час виконання мовою програмування

Деякі плати для розробки Інтернету речей використовують певну вбудовану підтримують додатки JavaScript, а плати Pycom WiPy підтримують розробку Python.

В порівнянні з рішеннями без ОС або RTOS, IoT- пристрою на основі мови виконання є значно більше сумісними. Вони можуть підтримувати розробку додатків сторонніх виробників і динамічні оновлення програмного забезпечення пристрою (чи його частин) динамічним способом без необхідності повторного виконання усього мікропрограмного забезпечення.

На концептуальному і технічному рівнях облаштування Інтернету речей на основі мови виконання дуже схожі на ранні платформи розробки мобільних застосувань, такі як платформа Java 2, Micro Edition (J2ME). У J2ME, динамічне середовище виконання мови служило в якості переносимого рівня виконання, що дозволяло розробляти додатки сторонніх виробників і створювати зручні для розробників інтерфейси додатків. Такі

можливості використовують інтерактивний характер динамічних мов, дозволяючи гнучко інтерпретувати і виконувати код "на льоту", без компрометації безпеки середовища виконання і пристрою, що лежить в основі. В основному, додатки працюють в пісочному ящику, який забезпечує тільки обмежений доступ до основних функцій платформи.

На рівні реалізації облаштування Інтернету речей на основі мови виконання зазвичай мають під собою RTOS. У цьому сенсі ці пристрої можна розглядати як наступний еволюційний крок вгору від пристроїв, побудованих на архітектурі RTOS.

Технічні можливості і вимоги до пам'яті пристроїв, грунтованих на архітектурі мова-час виконання, значно розрізняються залежно від підтримуваних мов. Розмір і складність віртуальних машин також значно розрізняються. Минималистичные мови програмування, такі як Forth, можуть зажадати всього декілька десятків кілобайт динамічної пам'яті, тоді як для віртуальних машин Python або JavaScript потрібно щонайменше декілька сотень кілобайт або переважно декілька мегабайт оперативної пам'яті. Відповідно, мінімальний об'єм флэш-памяти або пам'яті ПЗП може також складати від декількох десятків кілобайт до декількох мегабайт. Проте пам'ять зберігання тепер настільки недорога, що її вартість лише трохи впливає на загальну ціну пристрою.

Архітектура повного OS

Наступним рівнем вище за архітектуру мови виконання є IoT-пристрої, які досить потужні для роботи повної OS (як правило, на базі Linux). Raspberry Pi є відмінним прикладом такого пристрою. Наявність повної ОС дає безліч переваг, таких як вбудована підтримка безпечної передачі файлів, призначених для користувача облікових записів, управління пристроями, оновлення ресурсів, зрілі інструментальні засоби розробки і багато інших функцій. Загальний характер пристроїв, що підтримують архітектуру з повною ОС, також дозволяє легко запускати різні типи

додатків і послуг сторонніх виробників, включаючи вищезгадані мовні застосування.

В порівнянні з архітектурою без ОС або RTOS, стеки з повною ОС мають значно більш високі вимоги до пам'яті і процесора. Наприклад, бажання запустити ОС на базі Linux в пристрої збільшує об'єм оперативної пам'яті з декількох десятків або сотень кілобайт (для вирішення на базі RTOS) до половини мегабайта як мінімум. Значно більш високі вимоги до енергоспоживання утрудняють використання таких пристроїв в тих випадках, коли потрібно роботу з леткими апаратами, за винятком систем, призначених для роботи з планшетами або ноутбуками, з місткістю батареї неменше декількох тисяч міліампер-годинників.

Архітектура OS додатка

На поточному високому рівні спектру облаштувань Інтернету речей знаходяться ношені платформи пристроїв, такі як Android Wear і Apple WatchOS. Ці платформи багато в чому порівнянні з платформами мобільних телефонів-застосувань від трьох до п'яти років тому. Вони надають багатоможливі платформи і API сторонніх розробників; Проте вони також значно збільшують мінімальні потреби в апаратних засобах. Наприклад, Android Wear і watchOS вимагають мінімум половини гігабайта (512 Мбайт) ОЗУ - більш ніж в 10 000 разів більше, ніж декілька десятків кілобайт ОЗУ, необхідних для простих облаштувань IoT- датчиків.

Вимоги до обчислювальної потужності облаштувань app - OS також різко вище, ніж в простих облаштуваннях IoT на базі мікроконтроллерів. Як правило, потрібно процесор класу ARM Cortex. Це обмежує максимальну тривалість автономної роботи декількома днями або тільки декількома годинами при інтенсивному використанні.

Архітектура контейнерного OS

Контейнер є автономним, портативним, виконуваним пакетом програмного забезпечення, що включає усе необхідне для його запуску: код, час виконання, системні інструменти, системні бібліотеки і налаштування.

Популярні реалізації включають Docker і CoreOS. Контейнери ізолюють додатки один від одного і базову інфраструктуру ОС, забезпечуючи при цьому додатковий рівень захисту для додатка. Це гарантує, що програмне забезпечення завжди працюватиме однаково незалежно від його фізичного середовища виконання. На технічному рівні контейнери фактично є легшим механізмом віртуалізації ОС. На відміну від віртуальних машин ОС, таких як Virtual Box або VMware Workstation, контейнери не віртуалізують повну гостьову ОС, а спільно використовують базову ОС з іншими контейнерами.

Враховуючи незалежність фізичного середовища виконання, яке можуть надати контейнери, вони також є привабливим вибором для розробки Інтернету речей, особливо у світлі сучасної технічної різноманітності облаштувань Інтернету речей. Таким чином, хоча контейнерні технології додають значні витрати в порівнянні з традиційним двійковим програмним забезпеченням, вони вже використовуються з облаштуваннями Інтернету речей. Наприклад, Docker вже можна використати в облаштуваннях Raspberry Pi.

З чисто технічної точки зору архітектура, грунтована на контейнерах, безперечно є життєздатним варіантом для облаштувань Інтернету речей за наявності достатньої пам'яті і інших ресурсів. Як мінімум, в середовищі хоста має бути доступне декілька гігабайт оперативної пам'яті, що робить цей підхід непридатним для переважної більшості сучасних облаштувань Інтернету речей. Хоча сьогодні облаштування Інтернету речей на основі контейнерів можуть здатися надмірними, ми бачимо в них важливий крок у напрямі повністю ізоморфної системної архітектури Інтернету речей, які ми обговорюємо в наступному розділі.

Більшість дослідників і експертів підтвердили, що забезпечення безпеки системи Інтернету речей є однією з найбільш серйозних проблем, облаштувань Інтернету речей, що перешкоджають успішному впровадженню. Цінність системи Інтернету речей полягає в тому, що вона об'єднує усі малі і великі системи і дозволяє їм спілкуватися один з одним

через Інтернет. Оскільки IoT - це динамічна система, в якій кожен погано захищений об'єкт може порушити безпеку і стійкість усієї системи, оскільки вони сполучені як ланцюжок. Простота підключення і доступу до облаштувань Інтернету речей відкриває двері для серйозних проблем безпеки, особливо при масштабному розподілі гетерогенних пристроїв, їх можливості підключення до інших пристроїв без запиту дозволів або навіть повідомлення їх власників, а також вірогідність затоплення цих пристроїв серйозними загрозами безпеки.

1.6 Переваги IoT

Представлені основні переваги Інтернету речей:

— Комунікація: IoT стимулює зв'язок між пристроями, також відомий як зв'язок "машина-машина" (M2M). Через це фізичні пристрої можуть залишатися підключеними, і, отже, повна прозорість доступна з меншою ефективністю і більш високою якістю.

— Автоматизація і контроль: завдяки тому, що фізичні об'єкти підключаються і управляються в цифровому і централізованому режимі за допомогою безпровідної інфраструктури, існує великий об'єм автоматизації і управління в роботі. Без втручання людини машини здатні спілкуватися один з одним, що призводить до швидшої реакції.

— Інформація: очевидно, що наявність більшої кількості інформації допомагає приймати кращі рішення. Незалежно від того, чи являються рішення уявні чи реальні.

— Монітор: найкраща перевага Інтернету речей - моніторинг. Знаючи точну кількість предметів постачання або якість повітря у вашому будинку, може додатково надати більше інформації, яка раніше не могла бути легко зібрана.

— Час: час, заощаджений завдяки IoT, може бути досить великим. І в сучасному житті ми усі могли б використати більше часу.

— Гроші: найбільша перевага Інтернету речей - економія грошей. Якщо ціна речей для маркування і моніторингу буде менше суми заощаджених грошей, то інтернет речей буде широко використовуватися. Автоматизація повсякденних завдань: приводить до кращого моніторингу пристроїв Інтернет речей дозволяє автоматизувати і контролювати щоденні завдання, уникаючи втручання людини. Обмін даними між машинами допомагає підтримувати прозорість процесів. Це також призводить до одноманітності завдань. Можливо підтримувати якість обслуговування і вжити необхідні заходи у разі надзвичайних ситуацій.

— Ефективність: отже, взаємодія між машинами забезпечує кращу ефективність; точні результати можуть бути отримані швидко. Це призводить до заощадження цінного часу. Замість того, щоб щодня повторювати одні і ті ж завдання, це дозволяє людям виконувати інші необхідні задачі.

— Економія коштів: оптимальне використання енергії і ресурсів може бути досягнуто за рахунок впровадження цієї технології і збереження пристроїв під спостереженням та бути попередженими про збої і ушкодження системи. Отже, ми можемо заощадити гроші, використовуючи цю технологію. [6]

1.7 Недоліки IoT

Представлені основні недоліки Інтернету речей:

— Сумісність: на даний момент немає стандарту для маркування і моніторингу за допомогою датчиків.

— Складність: існує декілька можливостей для відмови складних систем.

— Конфіденційність: конфіденційність є великою проблемою для Інтернету речей. Усі дані мають бути зашифровані так, щоб дані про ваш

фінансовий стан або про те, скільки молока ви споживаєте, не були загальновідомі ні на робочому місці, ні з друзями.

— Безпека: є вірогідність, що програмне забезпечення може бути зламане і ваша особиста інформація використовується неправильно. Отже, усі риски безпеки стають обов'язком споживача. [6]

1.8 Безпека IoT

Більшість дослідників і експертів підтвердили, що забезпечення безпеки системи Інтернету речей є однією з найбільш серйозних проблем, облаштувань Інтернету речей, що перешкоджають успішному впровадженню. Цінність системи Інтернету речей полягає в тому, що вона об'єднує усі малі і великі системи і дозволяє їм спілкуватися один з одним через Інтернет.

Оскільки IoT - це динамічна система, в якій кожен погано захищений об'єкт може порушити безпеку і стійкість усієї системи, оскільки вони сполучені як ланцюжок. Простота підключення і доступу до облаштувань Інтернету речей відкриває двері для серйозних проблем безпеки, особливо при масштабному розподілі гетерогенних пристроїв, їх можливості підключення до інших пристроїв без запиту дозволів або навіть повідомлення їх власників, а також вірогідність затоплення цих пристроїв серйозними загрозами безпеки. Рішення проблем безпеки в контексті Інтернету речей має бути основним пріоритетом для ширшого впровадження додатків Інтернету речей. Користувачі мають бути повністю упевнені у безпеці своїх облаштувань Інтернету речей і пов'язаних з ними застосувань. Вони повинні забезпечити повний захист своїх пристроїв від різних відомих загроз, оскільки вони стають більше інтегрованими в повсякденне життя людей.

Основні вимоги безпеки для Інтернету речей

Безпеку системи Інтернету речей можна оцінити за допомогою класичних заходів безпеки і аналізу ризиків. У системі Інтернету речей повинні використовуватися типові вимоги до безпеки ЦРУ (конфіденційність, цілісність і доступність). Конфіденційність означає, що обмін повідомленнями між посилачем і одержувачем має бути захищений від будь-якого шкідливого або непідтвердженого користувача. Для системи Інтернету речей конфіденційність повинна гарантуватися не лише усередині мережі зв'язку, але і при передачі повідомлень між різними облаштуваннями Інтернету речей. Цілісність використовується для того, щоб гарантувати зміст повідомлень, що передаються між посилачем і одержувачем, яке захищене від будь-яких маніпуляцій з боку зловмисника, без того, щоб одержувач міг відстежувати цю маніпуляцію.

У системі Інтернету речей перевірка цілісності може виконуватися на кожному вузлі, що бере участь в обміні повідомленнями між посилачем і одержувачем. Доступність використовується для гарантії того, що шкідливий користувач нездатний порушити або шкідливо вплинути на зв'язок або якість послуг, IoT, що надаються, пристроями або мережею зв'язку. Хоча ЦРУ має важливе значення для Інтернету речей, для кожного рівня архітектури Інтернету речей потрібні інші вимоги до безпеки. Аутентифікація вузла є основною проблемою безпеки для фізичного рівня, щоб уникнути несанкціонованого доступу до вузла і захистити канал зв'язку між вузлами IoT від будь-яких атак. Полегшений криптографічний алгоритм і протокол є важливим аспектом шифрування передаваних даних, особливо для облаштувань Інтернету речей з обмеженими ресурсами. (рис. 1.4)

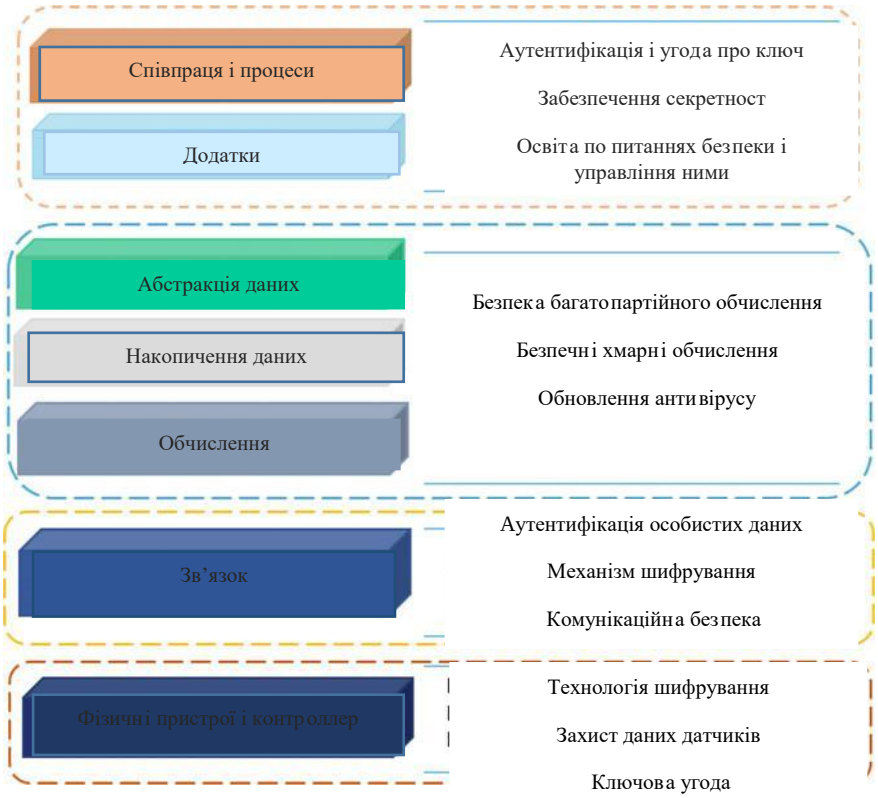

Рис. 1.4 Основні рівні архітектури Інтернету речей

Для підключення або мережевого рівня потрібні заходи безпеки зв'язку, а також аутентифікація ідентифікаційних даних для відвертання незаконних вузлів. Крім того, на цьому рівні поширена розподілена атака з відмовою в обслуговуванні (DDoS), тому існує необхідність захисту від DDOS - атаки у беззахисних вузлах цього рівня, особливо в контексті Інтернету речей. Для абстракції даних, накопичення і граничних обчислень потрібні багато механізмів захисту додатків для захисту даних, що зберігаються в хмарних обчисленнях. Окрім оновленого антивіруса потрібні сильні алгоритми шифрування. Тоді як для рівня додатків і спільної роботи необхідно прийняти угоду про перевірку достовірності і ключ для захисту конфіденційності користувача. Крім того, освіта і управління паро лями мають важливе значення для інформаційної безпеки на цьому рівні.

Новий підхід, запропонований для реалізації необхідних заходів безпеки впродовж життєвого циклу розробки програмного забезпечення і устаткування, а не після виявлення порушення безпеки. Для захисту мільярдів облаштувань Інтернету речей, які погано захищені від звичайних

атак на систему безпеки, необхідно використати систему безпеки за допомогою дизайну. Оскільки ці пристрої підключені до Інтернету, вони стають слабким місцем, яке може бути використане будь-яким зловмисником безпеки для крадіжки сенсорної інформації або порушення роботи сервісу. Крім того, більшість цих пристроїв були вбудовані в систему без забезпечення безпеки, що зробило їх легкими мішенями для зловмисників.

Даний підхід спрямований на захист безпеки більшості пристроїв. Інформованість користувачів про безпеку довела, що вона створює безліч уязвимостей і загроз, які можуть вплинути на життя людей, але підхід спрямований на допомогу користувачеві зрозуміти вимоги до безпеки Інтернету речей і спонукати його прийняти правильні рішення для забезпечення своєї безпеки.

Передові практики захисту технологій Інтернету речей

Проблеми безпеки Інтернету речей, створюють потенційні ризики в нашому житті. Порушення безпеки може привести до втрати ваших грошей, але за допомогою Інтернету речей атака безпеки може буквально привести до втрати вашого життя. Захист Інтернету речей вимагає застосування набору передових практик, що включають наступне:

— Апаратний захист від несанкціонованого доступу: збереження ізольованих облаштувань Інтернету речей, і тільки деякі люди мають фізичний доступ до них, є основними кроками, щоб захистити Інтернет речей від несанкціонованого доступу або індикації несанкціонований доступу. Крім того, зміцнення безпеки завдяки фізичній безпеці, такій як блокування невживаних портів і вимкнутої камери, є хорошим етапом для відвертання доступу потенційних зловмисників до ваших даних.

— Надійна аутентифікація: багато користувачів Інтернету речей як і раніше використовують прості паро лі і паро лі за умовчанням без яких-небудь оновлень. Перед використанням пристрою виробники повинні попросити клієнта оновити паро ль за умовчанням за допомогою надійних

паро лів. Крім того, потрібні альтернативні способи розпізнавання ідентифікаційних даних, оскільки ім'я користувача і паро ль не є реалістичними для кожного пристрою.

— Оновлення ПО: налаштування системи повинно мати можливість установки або регулярні оновлення. У Інтернеті є декілька серйозних загроз, які впливають на Інтернет речей. Постачальники послуг повинні планувати майбутні оновлення програмного забезпечення пристроїв, щоб підтримувати його в актуальному стані. Ці оновлення повинні виконуватися на тимчасовій основі або з урахуванням необхідності оновлення.

— Динамічне тестування: необхідно пройти тестування і створити найменш стандартні заходи безпеки. Для перевірки безпеки Інтернету речей існують два типи: статичний і динамічний. На відміну від статичного тестування, пов'язаного з виявленням загроз в програмному забезпеченні, динамічне тестування може досліджувати загрози і можливості як апаратного, так і програмного забезпечення.

— Проектування аварійного перемикання на резервний ресурс: даний єтап повинен працювати належним чином у разі втрати або похибки підключення до Інтернету. Проте для роботи з такими властивостями, як безперервність Інтернету або роз'єднання даних, створено мало налаштувань безпеки Інтернету речей. Конструкція аварійного перемикання на резервний ресурс потрібна для користувачів, наприклад як механізми блокування дверей, відеомонітор, монітори і аварійні сигнали довкілля. Ці пристрої повинні мати додаткові функції при відключених операціях.

Висновки:

В першому розділі було розв’язано такі питання:

— Розглянуто основні терміни мережі Інтернет речей;

— Досліджено архітектуру та основні компоненти IoT. Наведено характеристики всіх основних елементів;

— Розглянуто еталону модель;

— Розглянуто безпеку і захисти безпеки IoT;

— Наведено переваги та недоліки, які притаманні мережам IoT;

— Після аналізу переваг та недоліків моделі IoT можна зробити висновок, що попри те, що переваг набагато більше ніж недоліків, на даний момент повноцінне використання Інтернет речей можливе з повними захистами безпеки та конфіденційності.

РОЗДІЛ 2
АНАЛІЗ ПЛАТФОРМ І СИСТЕМ МОНІТОРИНГУ ТРАФІКУ НА АВТОШЛЯХАХ

2.1 Базові визначення моніторингу

Сучасні комп'ютерні системи побудовані на мережі Internet, або об'єднані в локальну мережу з подальшим виходом до Internet. Ураховуючи сучасний стан інформаційних і комунікаційних технологій для концентрації інформації щодо комп'ютерних мереж постає проблема моніторингу.

Моніторинг - систематичний збір і обробка інформації, яка може бути використана для поліпшення процесу ухвалення рішення, а також побічно для інформування громадськості або прямо як інструмент зворотного зв'язку в цілях здійснення проектів, оцінки програм або вироблення політики. Він несе одну або більш з трьох організаційних функцій:

— Виявляє стан критичних або таких, що знаходяться в стані зміни явищ середовища, відносно яких буде вироблений курс дій на майбутнє;

— Може допомогти встановити відносини з своїм оточенням, забезпечуючи зворотний зв'язок, відносно попередніх успіхів і невдач певної політики або програм;

— Може бути корисний для встановлення відповідності правилам і контрактним зобов'язанням.

Існує ряд програм мережевого моніторингу:

Програма ping, програма ipconfig, сервери SNMP, Zabbix (Open Source), NetXMS (Open Source), Big Brother, Optivity, Caligare Flow Inspector, MRTG, RRDtool, Intellipool Network Monitor, Ipswitch WhatsUp, ManageEngine OpManager, Netmon — Appliance based network monitoring suite with email and pager alert system, Cricket, PRTG, Packet Analyzer: Network Traffic Monitoring, Analysis and Troubleshooting, NetVizor, NetDecision, HP OpenView Network Node Manager (NNM), Cisco Works NMS.

Підсистеми, з яких складається моніторинг мережі

Процес контролю роботи мережі зазвичай ділять на два етапи - моніторинг і аналіз.

На етапі моніторингу виконується більш проста процедура - процедура збору первинних даних про роботу мережі: статистики про кількість циркулюючих в мережі кадрів і пакетів різних протоколів, стан портів концентраторів, комутаторів і маршрутизаторів і т. п.

Далі виконується етап аналізу, під яким розуміється більш складний і інтелектуальний процес осмислення зібраної на етапі моніторингу інформації, зіставлення її з даними, отриманими раніше, і вироблення припущень про можливі причини сповільненої або ненадійної роботи мережі.

Завдання моніторингу вирішуються програмними і апаратними вимірниками, тестерами, мережевими аналізаторами, вбудованими засобами моніторингу комунікаційних пристроїв, а також агентами систем управління. Завдання аналізу вимагає більш активної участі людини і використання таких складних засобів, як експертні системи, що акумулюють практичний досвід багатьох мережевих фахівців.

Всі засоби моніторингу та аналізу мереж, можна розділити на кілька великих класів:

— Системи управління мережею (Network Management Systems) - централізовані програмні системи, які збирають дані про стан вузлів і комунікаційних пристроїв мережі, а також дані про трафік в мережі. Ці системи не тільки здійснюють моніторинг і аналіз, а й виконують в автоматичному чи напівавтоматичному режимі управління мережею - включення і відключення портів пристроїв, зміна параметрів мостів адресних таблиць мостів, комутаторів і маршрутизаторів і т.п. Прикладами систем управління можуть служити популярні системи HPOpenView, SunNetManager, IBMNetView, Cacti та інші.

— Засоби управління системою (System Management). Засоби управління системою часто виконують функції, аналогічні функціям систем управління, але стосовно інших об'єктів. У першому випадку об'єктом управління є програмне і апаратне забезпечення комп'ютерів мережі, а у другому - комунікаційне устаткування. Разом з тим, деякі функції цих двох видів систем управління можуть дублюватися, наприклад, засоби управління системою можуть виконувати найпростіший аналіз мережевого трафіку. До найбільш відомих систем управління системами відносяться LANDesk, IBM Tivoli, Microsoft Systems Management Server, HP OpenView, Novell ZENworks і CA Unicenter.

— Вбудовані системи діагностики і управління (Embedded Systems). Ці системи виконуються у вигляді програмно-апаратних модулів, які встановлюються в комунікаційне обладнання, а також у вигляді програмних модулів, вбудованих в операційні системи. Вони виконують функції діагностики і управління тільки одним пристроєм, і в цьому їх основна відмінність від централізованих систем управління. Прикладом засобів цього класу може служити модуль управління концентратором Distrebuted 5000, котрий реалізує функції автосигментації портів при виявленні несправностей, приписування портів внутрішнім сегментам концентратора і деякі інші. Як правило, вбудовані модулі управління також виконують роль SNMP-агентів, які поставляють дані про стан пристрою системам управління.

— Аналізатори протоколів (Protocol analyzer). Представляють собою програмні або апаратно-програмні системи, які обмежуються на відміну від систем управління лише функціями моніторингу і аналізу трафіку в мережах. Хороший аналізатор протоколів може захоплювати і декодувати пакети великої кількості протоколів, що застосовуються в мережах - зазвичай кілька десятків. Аналізатори протоколів дозволяють встановити деякі логічні умови для захоплення окремих пакетів і виконують повне

декодування захоплених пакетів, тобто показувати в зручній для користувача формі вкладеність пакетів протоколів різних рівнів один в одного з розшифруванням змісту окремих полів кожного пакета.

— Обладнання для діагностики і сертифікації кабельних систем. Умовно це устаткування можна поділити на чотири основні групи: мережні монітори, прилади для сертифікації кабельних систем, кабельні сканери і тестери (мультиметри). Мережеві монітори (називають також мережевими аналізаторами) призначені для тестування кабелів різних категорій. Слід розрізняти мережеві монітори і аналізатори протоколів. Мережеві монітори збирають дані лише про статистичні показники трафіку - середньої інтенсивності загального трафіку мережі, середньої інтенсивності потоку пакетів з певним типом помилки і т.п. Призначення пристроїв для сертифікації кабельних систем, безпосередньо випливає з їх назви. Сертифікація виконується відповідно до вимог одного з міжнародних стандартів на кабельні системи. Кабельні сканери використовуються для діагностики мідних кабельних систем. Тестери призначені для перевірки кабелів на відсутність фізичного розриву.

— Експертні системи. Цей вид систем акумулює людські знання про виявлення причин аномальної роботи мереж і можливі способи приведення мережі у працездатний стан. Експертні системи часто реалізуються у вигляді окремих підсистем різних засобів моніторингу та аналізу мереж: систем управління мережами, аналізаторів протоколів, мережевих аналізаторів. Найпростішим варіантом експертної системи є контекстно-залежна help-система. Більш складні експертні системи являють собою так звані бази знань, що володіють елементами штучного інтелекту. Прикладом такої системи є експертна система, вбудована в систему управління Spectrum компанії Cabletron.

— Багатофункціональні пристрої аналізу та діагностики. У зв'язку з розповсюдженням локальних мереж виникла необхідність розробки

недорогих портативних приладів, які суміщають функції декількох пристроїв: аналізаторів протоколів, кабельних сканерів і, навіть, деяких можливостей ПЗ мережного управління. Як приклад такого роду пристроїв можна привести Compas компанії Microtest Inc. або 675 LAN Meter компанії FlukeCorp

Моніторинг мережі складається з декількох окремих підсистем, зокрема:

а) система виявлення вторгнень (Intrusion Detection System, IDS) – слідкує за появою зовнішніх загроз;

б) система моніторингу продуктивності мережі (Network Performance Monitoring, NPM) виявляє перезавантажені вузли та канали;

в) система моніторингу мережі (Network Monitoring System, NMS) виконує спостереження за мережею в пошуках проблем, що викликані серверами або іншими пристроями чи мережними з’єднаннями, що вийшли з ладу.

Система виявлення вторгнень (IDS) - це пристрій або програмний додаток, який відстежує мережу або системи на предмет шкідливих дій або порушень політики. Про будь-які дії або порушеннях вторгнення зазвичай повідомляють або адміністратору, або збирають централізовано з використанням системи захисту інформації та управління подіями (SIEM). Система SIEM об'єднує вихідні дані з декількох джерел і використовує методи фільтрації аварійних сигналів, щоб відрізнити шкідливу активність від помилкових аварійних сигналів.

Система моніторингу ефективності мережі (NPM) - це рішення в Operations Management Suite, яке відстежує продуктивність мережі між офісними майданчиками, центрами обробки даних, хмарами і додатками практично в режимі реального часу. Він допомагає адміністратору знаходити і усувати вузькі місця, такі як затримка в мережі, втрата даних і доступність будь-якого мережевого з'єднання через локальні мережі, віртуальні мережі

Microsoft Azure, віртуальні віртуальні машини Amazon Web Services, гібридні мережі, VPN або навіть загальнодоступні інтернет-з'єднання.

Система моніторингу мережі - це система, призначена для моніторингу, обслуговування та оптимізації мережі. Вона включає в себе як апаратне, так і програмне забезпечення, але частіше за все NMS відноситься до програмного забезпечення, що використовується для управління мережею. Системи управління моніторингом мережею надають наступні можливості:

— Моніторинг мережі - програмне забезпечення NMS забезпечує контроль мережевого обладнання, щоб бачити, що всі пристрої працюють правильно і працюють не на повну або на повну потужність. В разі виявлення проблеми на мережі, адміністраторам можуть бути відправлені відповідні сповіщення.

— Виявлення пристрою - коли новий пристрій (вузол) підключається до мережі, NMS виявляє його, щоб його можна було розпізнати, налаштувати і додати в мережу. Це також називається підготовкою пристрою до підключення в дану мережу.

— Аналіз продуктивності - NMS може вимірювати поточну і попердню (history) продуктивність мережі. Вона включає в себе загальну продуктивність мережі, а також окремих пристроїв і підключень. Наприклад, NMS може виявляти аспекти мережі, де пропускна здатність наближається до максимально допустимої в смузі пропускання. Дані можуть використовуватися для оптимізації потоку трафіку і засвідчувати про необхідність додавання нового обладнання при необхідності.

— Управління пристроями (вузлами) NMS може надати простий спосіб управління декількома пристроями з центрального місця розташування. Він може використовуватися для настройки пристрою або зміни налаштувань на основі аналізу продуктивності. Прикладом може бути: можливість включати активацію певних мережевих портів на комутаторі або реалізацію регулювання смуги пропускання для певних пристроїв.

— Управління збоями. Якщо відбувається збій пристрою або розділу мережі, NMS може автоматично перенаправляти трафік для обмеження часу простою. Ця дія може бути виконана на в реальному часі (відразу) або може бути виконана з використанням набору попередньо налаштованих правил. При виникненні помилки мережеве попередження або повідомлення зазвичай відправляється одному або декільком мережевим адміністраторам.

Платформи систем моніторингу

ZABBIX – це вільна система моніторингу та відстеження статусів різноманітних сервісів комп'ютерних мереж, що містять UNIX-подібні чи Windows хости, серверів та мережевого обладнання. (рис 2.1)

Моніторинг великої кількості пристроїв вимагає в допомогу інструменти автоматизації, інакше складно проводити «вручну» налаштування параметрів моніторингу для великої кількості вузлів, до того ж завжди є можливість допустити помилку. Zabbix має набір інструментів для автоматизації: це шаблони, виявлення мережевих пристроїв, автореєстрація Zabbix-агентів. [9]

Також дана система дозволяє проводити веб-моніторинг. Для активації веб-моніторингу необхідно створити веб-сценарії. Сценарій станів з одного або декількох запитів HTTP або "кроків". Зібрані дані з виконання вебсценаріїв зберігаються в базі даних. Ці дані автоматично використовуються для графіків, тригерів і оповіщень.

Серед основних можливостей системи моніторингу Zabbix можна виділити наступні:

— Розподілений моніторинг до 1000 вузлів;

— Сценарії на основі моніторингу;

— Централізований моніторинг лог-файлів (перевірка файлів реєстрації на помилковість);

— Автоматичне виявлення (автоматичне виявлення за діапазоном IPадрес і SNMP-перевірка);

— SLA (Service Level Agreement) моніторинг (регулювання взаємовідносин між підрозділами організацій, перелік параметрів якості тощо);

— Комплексна реакція на події;

— Гнучка система шаблонів і груп;

— Можливість створювати карти мереж

Дана система моніторингу сьогодні дуже часто використовується компаніями, вона є безкоштовною, але для правильного сконфігурування потрібно задіяти багато зусиль.

OpenView є всеосяжним рішенням з управління IT-інфраструктурою підприємства будь-якого розміру і напрямку діяльності. Побудовано на основі модульної архітектури. Надає широкі можливості з моніторингу та управління локальними обчислювальними мережами, серверними платформами (такими як HP-UX, Solaris, AIX, Novell, Linux, весь спектр Windows-платформ), додатками (SAP, Oracle, Sybase, MS SQL, Exchange, DB2, Informix, MS Active Directory, ...), робочими місцями користувачів (інвентаризація, віддалена установка ОС, оновлень, програмного забезпечення, налаштувань користувачів, контроль за використанням ПЗ), організація диспетчерської служби ті інше.

Cacti - open-source веб-додаток, система дозволяє будувати графіки за допомогою RRDtool. Cacti збирає статистичні дані за певні часові інтервали і дозволяє відобразити їх у графічному вигляді. Переважно використовуються стандартні шаблони для відображення статистики по завантаженню процесора, виділенню оперативної пам'яті, кількістю запущених процесів, використання вхідного / вихідного трафіку. Прикладом використання можу навести: мобільні оператори часто використовують Cacti для збирання даних про трафік мережі і подальший її моніторинг.

Рис. 2.1. Платформи моніторингу трафіку ZABBIX, OpenView, Cacti

2.2 Моніторинг руху

У зв'язку з урбанізацією числа доріг, транспортні засоби нестримно ростуть. Моніторинг руху і контроль за ним кидають виклик багатьом містам нашої країни. Більшість міст досі страждають від пробок і пов'язаних з ними проблем. У зв'язку з цим виникає безліч проблем, таких, як затримка в русі між двома великими містами, витрата палива на перехрестях, забруднення повітря із-за викидів, загибель людей на дорогах в результаті аварій і багато проблем, пов'язаних з транспортом. Дослідження показують, що 30% викидів діоксиду доводиться на транспортні системи, неефективне управління дорожнім рухом призводить до витрати палива у розмірі мільярда галонів в рік, також погано розроблені сигнали дорожнього руху призводять до збоїв в русі і збільшенню затримок. Великі міста пов'язані швидкісними автомагістралями, які призводять до загибелі людей в ДТП через кількість транспортних засобів і підвищують їх швидкість на автомагістралях.

Останніми роками дорожньо-транспортні події, в яких брали участь багато учасників дорожнього руху (транспортні засоби, пішоходи, тварини) і які привели до жертв із смертельним результатом і більш ніж серйозних травм, якими нехтують люди і державні органи. Для вирішення таких проблем на автомагістралях потрібно інтелектуальні системи управління дорожнім рухом і органи влади, які можуть здійснювати моніторинг руху в режимі реального часу і стану руху на перехрестях в містах. Цей системний процес необхідно виконати впродовж 24 * 7 годин для перевірки стану

трафіку на дорогах і управління їм, що може бути зроблено за допомогою технології Інтернету віщої (Internet of Things) і безпровідної технології.

Транспортні засоби, системи датчиків на стороні дороги і допоміжні системи дорожньої інфраструктури збирають повсякденну інформацію про умови дорожнього руху. Встановлені дорожні бічні системи зазвичай призначені для незалежної роботи і забезпечення вимірів тільки обмеженим числом кінцевих користувачів. Зазвичай забезпечує технічне обслуговування доріг. Окрім систем датчиків сторони дороги, нові транспортні засоби оснащені декількома системами датчиків допомоги водієві, які вимірюють довкілля поза транспортним засобом. Інформація про датчики для водія з середовища руху обмежена датчиками автомобілів, хоча нові мобільні телефони і навігатори здатні отримувати інформацію практично в режимі реального часу. Крім того, доступні нові комунікаційні технології, такі як стандарт IEEE 802.11 для зв'язку між транспортними засобами. [10]

Таким чином, кожен сервіс, що розробляється у реальному світі, має бути поміщений у відповідний осередок хмари, яка об'єднує близькі по функціональності і корисні людині компоненти. Уже реалізовані масштабні проекти, покликані вирішити проблеми, що створилися. Це спеціалізовані системи автоматизованого моніторингу дорожнього руху OnStar, NEXCO Central, ECall Japan, ECall Europe. Також розглянемо такі системи як: система аналізу дорожнього руху (RTA), Моха та система моніторингу дорожнього руху в режимі реального часу з використанням алгоритму SAR**.** Виокремлені основні переваги і недоліки кожної з систем, що дозволяє прийняти правильні інтеграційні архітектурні рішення для внесення абсолютно рішучих змін системи моніторингу дорожнього руху і управління транспортом, що оптимізує виконання транспортних маршрутів усіма учасниками дорожнього руху.

У зв'язку з урбанізацією числа доріг, транспортні засоби нестримно ростуть. Моніторинг руху і контроль за ним кидають виклик багатьом містам нашої країни. Більшість міст досі страждають від пробок і пов'язаних з ними

проблем. У зв'язку з цим виникає безліч проблем, таких, як затримка в русі між двома великими містами, витрата палива на перехрестях, забруднення повітря із-за викидів, загибель людей на дорогах в результаті аварій і багато проблем, пов'язаних з транспортом. Дослідження показують, що 30% викидів діоксиду доводиться на транспортні системи, неефективне управління дорожнім рухом призводить до витрати палива у розмірі мільярда галонів в рік, також погано розроблені сигнали дорожнього руху призводять до збоїв в русі і збільшенню затримок. Великі міста пов'язані швидкісними автомагістралями, які призводять до загибелі людей в ДТП через кількість транспортних засобів і підвищують їх швидкість на автомагістралях.

Останніми роками дорожньо-транспортні події, в яких брали участь багато учасників дорожнього руху (транспортні засоби, пішоходи, тварини) і які привели до жертв із смертельним результатом і більш ніж серйозних травм, якими нехтують люди і державні органи. Для вирішення таких проблем на автомагістралях потрібно інтелектуальні системи управління дорожнім рухом і органи влади, які можуть здійснювати моніторинг руху в режимі реального часу і стану руху на перехрестях в містах. Цей системний процес необхідно виконати впродовж 24 * 7 годин для перевірки стану трафіку на дорогах і управління їм, що може бути зроблено за допомогою технології Інтернету віщої (Internet of Things) і безпровідної технології.

Транспортні засоби, системи датчиків на стороні дороги і допоміжні системи дорожньої інфраструктури збирають повсякденну інформацію про умови дорожнього руху. Встановлені дорожні бічні системи зазвичай призначені для незалежної роботи і забезпечення вимірів тільки обмеженим числом кінцевих користувачів. Зазвичай забезпечує технічне обслуговування доріг. Окрім систем датчиків сторони дороги, нові транспортні засоби оснащені декількома системами датчиків допомоги водієві, які вимірюють довкілля поза транспортним засобом. Інформація про датчики для водія з середовища руху обмежена датчиками автомобілів, хоча нові мобільні телефони і навігатори здатні отримувати інформацію практично в режимі

реального часу. Крім того, доступні нові комунікаційні технології, такі як стандарт IEEE 802.11 для зв'язку між транспортними засобами.

Таким чином, кожен сервіс, що розробляється у реальному світі, має бути поміщений у відповідний осередок хмари, яка об'єднує близькі по функціональності і корисні людині компоненти. Уже реалізовані масштабні проекти, покликані вирішити проблеми, що створилися. Це спеціалізовані системи автоматизованого моніторингу дорожнього руху OnStar, NEXCO Central, ECall Japan, ECall Europe. Виокремлені основні переваги і недоліки кожної з систем, що дозволяє прийняти правильні інтеграційні архітектурні рішення для внесення абсолютно рішучих змін системи моніторингу дорожнього руху і управління транспортом, що оптимізує виконання транспортних маршрутів усіма учасниками дорожнього руху.

Система моніторингу транспортних засобів OnStar

Система моніторингу транспортних засобів OnStar Система розроблена компанією OnSatr Corporation, заснованою в 1995 році. На самому початку становлення компанії продавала окремі пристрої, які були доступні тільки власникам певних моделей автомобілів: Cadillac DeVille, Cadillac Seville і Cadillac Eldorado. До 2005 року OnStar сервіси сталі доступні власникам автомобілів декількох найбільш поширених марок: Acura, Audi, Isuzu, Subaru, Volkswagen. Варто відмітити, що до цього часу пристрою поступили в серійне виробництво і встановлювалися в автомобілі на етапі складання. У квітні 2006 року вже налічувалося 500 000 користувачів системи. У 2009 році компанія вийшла на Китайський ринок. На даний момент налічується близько 4 000 000 користувачів цього сервісу. [7]

Основні технології, які використовуються для моніторингу транспортних засобів. Система використовує CDMA канал зв'язку, що надається переважно Verizon Wireless і Bell Mobility. Для визначення місця розташування використовується GPS. Є можливість голосового зв'язку з операторами. Інформація з сенсорів (в основному це датчики ударів і

спрацьовування подушок безпеки) автоматично передається в call- центри. Це дозволяє негайно оповістити про місце розташування аварії рятувальні і правоохоронні органи. Окрім цього, усі машини, обладнані цією системою, мають GPS передавач, який дозволяє відстежити викрадений автомобіль. Також є можливість отримання інформації про швидкість, витрату палива і напрям руху. Це дозволяє зробити висновки про стиль водіння автомобіля. Нові моделі автомобілів обладнані системою віддаленої зупинки двигуна. Після такої зупинки автомобіль можна завести тільки після введення спеціального секретного коду.

Користувачі можуть застосовувати різні тарифні плани:

а) Тариф включає автоматичне сповіщення про аварію, моніторинг викраденого автомобіля, аварійні сервіси (виклик евакуатора, пересувний СТО) в не зони покриття мобільної мережі, а також віддалену діагностику транспортного засобу (дозволяє вирішити незначні проблеми за допомогою інструкцій call- центру).

б) Тариф ключає усі перелічені вище сервіси. Додатково є можливість моніторингу напряму руху і стилю водіння автомобіліста.

Система моніторинга дорожнім рухом NEXCO Central

Система розроблена Japan Highway Public Corporation. Принцип роботи полягає в глобальному моніторингу дорожнього руху на головних автострадах країни. На даний момент система покриває близько 2000 км доріг. Система централізована і центр управління рухом знаходиться в Токіо. (рис 2.2) Датацентр обробляє величезну кількість даних, що отримуються з дорожніх датчиків з хвилинним інтервалом. Це забезпечує максимально реальну картину дорожньої ситуації**.**

Рис. 2.2 Центр управління дорожнім рухом в Японії

На дорогах встановлено 744 точки доступу, які дозволяють працювати аварійним телефонним каналам і датчикам на передачу необхідної інформації про дорожню ситуацію.

Для передачі даних використовується глобальна IP мережа, за допомогою якої інформація з датчиків поступає на монітори центру управління автошлахами. Глобальна передача даних забезпечується за допомогою оптоволоконних комунікацій. Це дозволяє швидко обробляти телефонні дзвінки і дані, що поступають. Розробники системи пропонують повний спектр послуг з розробки і впровадження подібної системи в інших країнах.

Створення системи управління дорожнім рухом, що дозволяє збирати, обробляти інформацію і використати отримані дані для вирішення поставлених проблем:

— Підготовка керівництва по реалізації: порядок дій для проектування системи та складання вимог ефективності функціонування системи;

— Розробка специфікації: створення специфікації пристроїв, необхідних для реалізації моделі;

— Реалізація: реалізація проекту та установка устаткування з розрахунком на максимальний термін служби елементів. Проведення тренінгів персоналу, спрямованих на підвищення швидкодії обробки запитів;

— Експлуатація: проведення тренінгів персоналу, спрямованих на підвищення швидкодії обробки запитів;

Система моніторинга дорожнім рухом ECall Японія

На дорогах була запущена інтелектуальна транспортна система, покликана здійснювати повну автоматизацію управління дорожнім рухом. На усі автомобілі стали встановлювати спеціальне бортове навігаційно-комунікаційне устаткування, за допомогою якого забезпечується контроль місця розташування і стану транспортного засобу. Передача інформації і сигналів, що управляють, а також дуплексний зв'язок з водієм здійснюється диспетчерською службою швидкого реагування під назвою Ecall. В результаті успішної діяльності системи смертність та завантаденність на дорогах Японії значно знизилась.

Вміст системи:

а) Вбудована система автомобіля: датчик удару, eCall пристрій, акселерометр;

б) Internet: GSM/3g/LTE, PSTN або IP мережа;

в) Call- центр: служби порятунку.

Система глобального моніторингу транспорту ECall Європа

З 2001 року країнами Євросоюзу також стала розроблятися програма eCall, згідно якої в 2015 році увесь автотранспорт, що продається на території співдружності, має бути укомплектований навігаційно-комунікаційними засобами, що спрацьовують при аварії та великому обсягу трафіку на дорогах, після чого по каналах GSM - зв'язку передається інформація про місцезнаходження автомобіля на найближчий диспетчерський пункт. [14](Рис 2.3)

Рис. 2.3 Архітектура системи ECall

Принцип роботи системи полягає в наступному - eCall автоматично активізується, коли датчики, які знаходяться усередині автомобіля, визначають велике скупчення машин або аварію. [15] Система набирає європейський номер, встановлюючи телефонне з'єднання з найближчим Call-центром, і відправляє дані або деталі події в службу, включаючи час події, точне місцерозташування автомобіля і напрям руху (особливо важливого на дорогах і в тунелях). eCall може також бути включений вручну, за допомогою натиснення кнопки в автомобілі. За деякими оцінками, eCall зможе прискорити час реагування на екстрені ситуації і на трафік машин взагалі на 40 % в міських регіонах і на 50 % в сільській місцевості, і рятувати до 2500 життів в рік. [11]

Система аналізу дорожнього руху (RTA)

Аналіз дорожнього руху (RTA) - найважливіший процес в управлінні дорожнім рухом. Правильно побудована система управління дорожнім рухом, грунтована на комплексному аналізі дорожнього руху, може збільшити пропускну спроможність існуючих автомагістралей.

Система аналізу дорожнього руху (RTA) включає ряд рішень, що складаються з наступних систем:

Система відеоспостереження - система дозволяє дистанційно спостерігати за ситуацією на автомагістралях. Система складається з камер відеоспостереження і спеціалізованого програмного забезпечення, призначеного для управління камерами і записуваними ними відеоданими, а також для взаємодії з іншими системами в рамках комплексу управління і

аналізу дорожнього руху. У нього також входить система інтелектуального аналізу відеоданих.

Засоби відображення і запису візуальної інформації - такі прилади призначені для ведення записів відеоданих, що надаються системою відеоспостереження, і для подальшої обробки таких відеоданих.

Система автоматичного розпізнавання номерних знаків - це система спостереження, що використовує метод оптичного розпізнавання символів (OCR) із зображень для прочитування номерних знаків автомобілів. Така система може використати стандартні відеокамери, призначені для системи відеоспостереження. Проте для забезпечення максимальної ефективності використовує спеціально розроблені камери.

Центральна диспетчерська станція – компонент, який включає створення спеціалізованої диспетчерської станції для дистанційного керування усіма системами, використовуваними для управління і контролю дорожнього руху.

Світлодіодні дорожні знаки і екрани даних зі змінною інформацією - ці компоненти спільно з іншими системами комплексу дозволяють оптимізувати рух автотранспортних засобів шляхом інформування водіїв про складні ділянки доріг або про зміни в умовах дорожнього руху на контрольованих автомагістралях. Усе це дозволяє понизити вірогідність пробок.

Система аналізу дорожнього руху дозволяє виконувати наступні завдання:

— Дистанційний контроль за рухом автотранспортних засобів на вуличних і автомагістралях;

— Спостереження за такими випадками, як ускладнення дорожнього руху в конкретних районах, дорожньо-транспортні події і порушення правил дорожнього руху;

— При необхідності оператор може отримати зображення з проблемної ділянки дороги дистанційно управляти дорожнім рухом за допомогою зміни режиму роботи світлофорів;

— Ухвалюють оперативні рішення про виклик відповідних органів або швидкій допомоги у разі дорожньо-транспортної події або у будь-яких інших проблемних ситуаціях;

— Сучасні комп'ютерні засоби аналізу зображень дозволяють автоматично збирати дані про дорожній рух і виявляти будь-які ускладнення дорожнього руху в конкретних районах, таких, як пробки, дорожньо-транспортні події і порушення правил дорожнього руху на проблемних ділянках автомагістралей і і перехрестях;

— Система відеоспостереження має територіально розподілену структуру для забезпечення однакових операцій управління і управління від центральної диспетчерської станції. Об'єкти оснащені цифровою системою відеоспостереження нового покоління на основі IP- технологій.

Така структура системи відеоспостереження забезпечує доступ до усіх пристроїв, працюючих усередині мережі. Крім того, система дозволяє переглядати відеоархіви з даними, видаленими з локальних облаштувань запису, і ідентифікувати параметри активації сигналізації. Основний напрямок робиться на можливість аналізувати надані камерами дані в автоматичному режимі зі своєчасними повідомленнями у відповідні органи у разі виникнення тривожної ситуації. Це дозволить ефективно контролювати великі території без необхідності збільшення чисельності персоналу відеоспостереження. Модулі аналізу відеоданих розташовані безпосередньо у відеокамер, і легко збільшує розміри системи відеоспостереження без необхідності установки яких-небудь додаткових серверів для обробки відеоданих. Система дозволяє встановити логічну послідовність для відображення зображення з камер відеоспостереження на відеоекрані оператора, а також зв'язати піктограми камери і відповідні вікна

відео з картами місця розташування і встановити параметри для активації сигналу тривоги. Також є можливість встановити маршрути патрулювання і можливість записувати усі події на мережевий дисковий простір і надавати доступ до відеоархівів з будь-якої точки усередині мережі впродовж заданого періоду часу. [12]

Параметри активації сигналу тривоги можуть бути встановлені на основі аналізу наступних подій:

— Контроль за автотранспортними засобами, припаркованими в місцях обмеженого користування;

— Контроль за автотранспортними засобами, що порушили правила дорожнього руху (здійснення повороту на обмеженій території; управління червоного світла; неправильне управління провулка;

— Перетин подвійної суцільної лінії; обмежене управління провулка; і так далі);

— Регулювання швидкості автомобіля;

— Контроль розмірів автотранспортних засобів;

— Система, працююча в автоматичному режимі, дозволяє операторам відеоспостереження просто дивитися через журнал тривожних подій, щоб знайти тип, дату і час тривожної події. Після цього оператори просто дивитимуться відеозапис відповідної події.

На основі отриманих даних оператори приймають рішення про вжиття відповідних заходів. Таке налаштування роботи операторів відеоспостереження дозволяє істотно понизити кількість непомітних подій.

Система моніторингу дорожнім рухом Моха

Дана система використовується постійно для зниження навантаження на дорогах, а особливо у вихідні дні і під час свят. В системі використовується декілька моніторів трафіку і центрів управління, щоб інформувати водіїв про ситуацію на дорогах і про альтернативні маршрути об'їзду. Для того, щоб отримувати інформацію в реальному часі, уздовж

шосе встановлена велика кількість камер. Більшість камер підтримують зум і обертання, і управляються моторчиком, який отримує команди по інтерфейсу. Використовуючи вже прокладені оптичні лінії уздовж шосе, інженери використали перетворювачі з оптики в інтерфейс для віддаленного управління камерами. Інтелектуальна транспортна система Моха. [8]

Перетворювачі з оптики в послідовний інтерфейс, як правило, використовуються в парах. Моха використовуж як автономні продукти, так і рішення для установки в шасі для систем високої щільності. У цьому проекті використовувалися перетворювачі з робочою температурою від - 40 до 85°C. В центрах управління була встановлена система, перевагою якої являється те, що 19 модулів можуть бути підключені до шасі, що дозволяє заощадити простір в шафі і спрощує підключення.

Основні переваги:

— Збільшення дальності зв'язку до 5 км з багатомодовим або 40 км з одномодовим оптичним волокном;

— Відсутність помилок і втрати даних із-за електричних перешкод;

— Промислове виконання дозволяє встановити перетворювачі у будь-якому місці;

— Компактне рішення дозволяє заощадити простір.

Система моніторингу дорожнього руху в режимі реального часу з використанням алгоритму SAR

Нині багато автомагістралей оснащені датчиками для спостереження за фактичною дорожньою ситуацією в цілях забезпечення безпеки дорожнього руху (щоб уникнути застою) і підвищення безпеки учасників дорожнього руху. На жаль, така детальна інформація про дорожній рух пропускається за межі основних автомагістралей через відсутність датчиків. Радари, що літають на великих висотах, забезпечують вирішення проблеми, щоб заповнити цей недолік, особливо якщо цю інформацію потрібно в разі аварій або катастроф, швидкого реагування на затори. Для цього розроблена

нова система радіолокації моніторингу руху. Система виконує складні завдання з придбання, обробки і доставки відповідних транспортних продуктів в спеціалізований центр управління рухом в режимі реального часу. Обробка SAR і GMTI виконується безпосередньо на борту літака. Із-за обмежень смуги пропускання тільки відповідні дані трафіку передаються на наземну станцію через термінал лазерного зв'язку або мікрохвильову низхідну лінію зв'язку. Після подальшої обробки дані передаються в центр управління трафіком.

Для виявлення транспортних засобів, що рухаються, і оцінки параметрів використовують вже існуючі GMTI- системи і алгоритми, створені у військовій області. Проте велика частина цих алгоритмів вимагає великих обчислювальних потужностей і, якщо обчислення повинні виконуватися в реальному часі, складність системи і витрати стають астрономічними. Для цілей моніторингу руху кожен транспортний засіб віднесений до певної дороги і відповідна база даних дорожнього руху. Крім того, немає необхідності виявляти транспортні засоби, що переміщаються по бездоріжжю. Отже, завдяки включенню апріорі відомої дорожньої мережі вже на етапі виявлення алгоритму GMTI і ігноруванню всього іншого, окрім транспортних засобів, що рухаються, то складність системи, витрати, а також обчислювальне навантаження значно понижені.

Дорожня мережа в основному використовується разом з алгоритмами GMTI. Ці алгоритми вимірюють азимутні зміщення транспортних засобів, що відбуваються із-за звичайного фокусування SAR, для обчислення швидкостей упоперек шляху. Дання обробка займає багато часу, оскільки в загальному випадку SAR зображення повинні генеруватися з урахуванням повної смуги пропускання, заданою частотою повторення імпульсів.

Алгоритм не вимагає фокусування SAR, оскільки працює на одно- або багатоканальних даних SAR. Геокодоване положення кожного транспортного засобу, що рухається, отримує безпосередньо з міжсекційної ділянки дорожньої осі з сигналом транспортного засобу, що рухається.

Обчислення параметрів руху здійснюють шляхом оцінки доплерівської частоти сигналу на перетині доріг. Параметри абсолютної швидкості, курсу і геокодованого положення оцінюються з високою точністю.

Алгоритм, який використовується в якості першого кроку апріорі відома дорожня вісь відображається в масив даних SAR з основним діапазоном. Необхідне координатне перетворення виконується таким чином, що географічні координати кожної дорожньої точки перетворяться у відповідні кодові числа центру променя в площині дальності/азимута. Положення центру променя виявленого транспортного засобу, що рухається, потім задається шляхом перетину сигналу транспортного засобу з відображеною точкою дороги (див. Рис. 2.4).

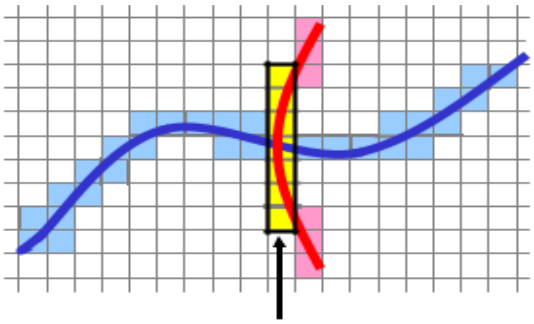

Рис. 2.4 Принцип алгоритму

Завдяки географічним координатам дорожньої точки і, отже, координати виявленого транспортного засобу, що рухається по цій дорожній точці під час центру променя. Для визначення швидкості переміщення і оцінки параметрів руху відбирають тільки декілька азимутних вибірок навколо точки перетину (див. Рис. 2.4 праву частину) і перетворять в доплерівську область за допомогою FFT. Черер невелике число використаних азимутних вибірок фаза сигналу є більш менш лінійною з часом, і тому сигнал транспортного засобу, що рухається, з'являється у вигляді різкого піку в доплерівській області. Для визначення амплітуди сигналу порівнюють з певним порогом і для оцінки параметрів руху використовують доплерівське зрушення піку сигналу. Пропонований алгоритм підходить лише для використання в повітрі, але не для космічних

цілей, оскільки характеристики виявлення страждають від низького SNR. [13]

Отримана продуктивність має на увазі, що алгоритм застосовний для додатків моніторингу трафіку в реальному часі.

2.3 Порівняльний аналіз розглянутих систем

Загальний аналіз перелічених вище систем моніторингу дорожнього руху дозволяє зрозуміти, що на сьогодні не існує комплексної системи, спрямованої на комплексне рішення поставленої проблеми. Жодна існуюча і жодна проектована система неприпускає наявності повного спектру послуг, спрямованого на підвищення комфорту автомобіліста і повного контролю трафіку на автошляхах. Йдеться або тільки про повний моніторинг автомобіля (OnStar, ECall,), або про глобальний моніторинг трафіку (NEXCO Centra, OnStar, система аналізу дорожнього руху (RTA), Моха та система моніторингу дорожнього руху в режимі реального часу з використанням алгоритму SAR) на основних і найжвавіших магістралях країни. Особливістю системи ECall є використання власних супутникових систем навігації. Проте ніщо не говорить про те, що застосування системи GPS (OnStar) менш ефективне. Основною перевагою супутникових систем навігації є велике покриття. Недоліки таких систем можна побачити в тунелях, підземних і багаторівневих магістралях. У такому разі потрібне введення наземних датчиків руху. Таке рішення пропонує японська система NEXCO Central. Також перевагою системи є відсутність необхідності установки спеціальних пристроїв на автотранспорт, проте такий підхід повністю виключає моніторинг окремих транспортних засобів. Основним недоліком цього підходу є обмежене покриття (тільки основні автомагістралі і траси).

Стосовно системи дорожнього руху RTA, то система дозволяє дистанційно спостерігати за ситуацією на автомагістралях та складається з камер відеоспостереження і спеціалізованого програмного забезпечення, призначеного для управління камерами і записуваними ними відеоданими, а

також для взаємодії з іншими системами в рамках комплексу управління і аналізу дорожнього руху, але можливе пошкодження данних або некорректне передання даних в реальному часі. Система контролю трафіку на завантажених дорогах Моха оснащена сучасним обладнням та технологіями, але обидві система не підтримується 24/7 повним контролем центру данних і це є основним недоліком данних системи.

Система моніторингу дорожнього руху в режимі реального час використовує радари, що літають на великих висотах, забезпечують вирішення проблеми, щоб заповнити цей недолік, особливо якщо цю інформацію потрібно в разі аварій або катастроф, швидкого реагування на затори. Для цього розроблена нова система радіолокації моніторингу руху, але система виконує складні завдання з придбання, обробки і доставки відповідних транспортних продуктів в спеціалізований центр управління рухом в режимі реального часу. Основним недоліком данної системи є неповний контроль вночі та кооштовне обладнання.

Послуги користувачам, які надає системи OnStar. Системи орієнтовані на забезпечення комфорту і безпеки як водія і пасажирів, так і самого транспортного засобу. Проте цим система і обмежена. OnStar не надає якій-небудь статистичній інформації про дорожню ситуацію. Також немає поняття централізованого управління. Система орієнтована тільки на окремі автомобілі, а нена транспортний потік.

Висновки:

В другій частині були розглянуті такі спеціалізовані системи автоматизованого моніторингу дорожнього руху: OnStar, NEXCO Central, ECall Japan, ECall Europe. Також розглянуто такі системи як: система аналізу дорожнього руху (RTA), Моха та система моніторингу дорожнього руху в режимі реального часу з використанням алгоритму SAR**.** Також розглянуто моніторинг і основні платформи для моніторингу трафіку, які використовуються в більшості країн світу. Таким чином, можна сказати, що

найбільш ефективним рішенням буде інтеграція розглянутих систем в одній універсальній. Це дозволить забезпечити автомобіліста повним спектром послуг, починаючи від ефективної навігації закінчуючи цілодобовим наданням інформації про автотранспортний засіб. Потрібно поліпшити інтегровану систему, ціль якої спрямована як на моніторинг кожного автомобіля окремо, так і на контроль дорожнього руху в цілому та зменщення наванатжень на дорогах, а саме повний контроль впорядку пріоритетності всього трафіку. Система має надавати можливість автоматизувати процеси оптимального управління транспортними засобами і дорожнім рухом в режимі реального часу для вирішення соціальних, гуманітарних, економічних і екологічних проблем.

РОЗДІЛ 3
ЗАСТОСУВАННЯ ІОТ ДЛЯ ДОСЛІДЖЕННЯ ТРАФІКУ НА АВТОШЛЯХАХ

3.1 Застосування IoT для дослідження трафіку на автошляхах

IoT дозволяє об'єктам взаємодіяти один з одним для отримання даних на веб-сервері, для зберігання і збору даних і для спільної роботи з користувачами. Таке розумне спілкування дає IoT без людської взаємодії.

Транспортні засоби, системи датчиків на дорогах і допоміжні системи дорожньої інфраструктури збирають повсякденну інформацію про умови дорожнього руху. Встановлені дорожні бічні системи зазвичай призначені для незалежної роботи і забезпечення вимірів тільки обмеженим числом кінцевих користувачів, але зазвичай забезпечує технічне обслуговування доріг.

Окрім систем датчиків на дорогах, нові транспортні засоби оснащені декількома системами датчиків допомоги водієві, які вимірюють довкілля поза транспортним засобом. Інформація про датчики для водія з середовища руху обмежена датчиками автомобілів, хоча нові мобільні телефони і навігатори здатні отримувати інформацію практично в режимі реального часу. Крім того, доступні нові комунікаційні технології, такі як стандарт IEEE 802.11p для зв'язку між транспортними засобами. [17]

Дана інтелектуальна система трафіку показує можливості об'єднання даних від транспортних засобів і надання їх кінцевим користувачам в зручному форматі. Стан дорожнього руху на дорогах і контроль за ним, що може бути зроблено за допомогою технології Інтернету речей (IoT) і безпровідної технології. Останні підходи, такі як технології зондування, використовується для моніторингу руху в реальному часі. За допомогою датчиків ми можемо визначити рівень руху на перехресті.

Спроектована система, що використовує мережу датчиків і збирає дані про стан рівня трафіку на смугах.. Це платформа, яка аналізує дані в режимі реального часу. Використовується сенсорна технологія для моніторингу

даних про рух транспортного засобу з використанням ультразвукових датчиків для визначення рівнів трафіку і передачі даних у блок контролера, який обробляє дані і відображає їх на сервері. Спосіб управління сигналом руху використовується для зменшення проблем руху і для пріоритету аварійного транспортного сигналу. Якщо на якій-небудь смузі високий рівень руху виявить тоді, то сигнал дасть більше часу для проходження транспортних засобів. Ця вбудована система, що використовує безпровідну мережу датчиків, забезпечує структуру для моніторингу і управління інформацією, пов'язаною з трафіком в реальному часі.[18]

3.2 Архітектура удосконалення контролю трафіку на автошляхах в порядку пріоритетності.

Ми пропонуємо для удосконалення контролю трафіку на автошляхах за допомогою технологій Інтернету речей. Архітектура підтримує функції збору, обробки, зберігання і передачі даних для усіх типів пристроїв і устаткування в середовищі Інтернету речей. Ця конструкція може широко використовувати IEEE1451.2 стандарт в якості посилання на доступ до декількох датчиків і перетворювачів. Стандарт передбачає ряд специфікацій від визначення інтерфейсу датчика до збору даних. Пропонована конструкція системи використовує IoT і безпровідну технологію для моніторингу трафіку в режимі реального часу. Масив ультразвукових датчиків, використовується для контролю рівня руху, які були обладнані на узбіччях доріг. Це придорожня інфраструктура, інтегрована з контролером, який передає дані на сервер через модуль Wi-Fi. Тут показана дорога, а саме перехрестя і на кожній дорозі були встановлені датчики на узбіччі дорогі для визначення рівнів руху по сигналу. Якщо спочатку смуга руху з більш високим рівнем руху, то пріоритет віддається цій смузі, тобто найвищому рівню руху, то більше часу для проходження транспортних засобів. Датчики на узбіччі дороги, інтегровані з блоком управління узбіччям дороги (RSU). [19]

Блок сторони дороги складається з блоку управління і контролю, блоку веб-сервера, модуля Wi-Fi, радіочастотних приймачів і системи пріоритету транспортного засобу. У сигналах алгоритм управління сигналом трафіку, використовуваний відповідно до визначення рівнів трафіку на доріжках ультразвуковими датчиками. Управління сигналами мікроконтролером здійснюється по виміру даних, які обробляються і передаються на сервер по модулю Wi-Fi. Радіочастотні приймачі використовуються для передачі і прийому даних з системи пріоритету транспортного засобу. Уся ця система змонтована з боку дороги, де використовувалася безпровідна сенсорна мережа. Загальна архітектура пропонованої системи показана на рис. 3.1

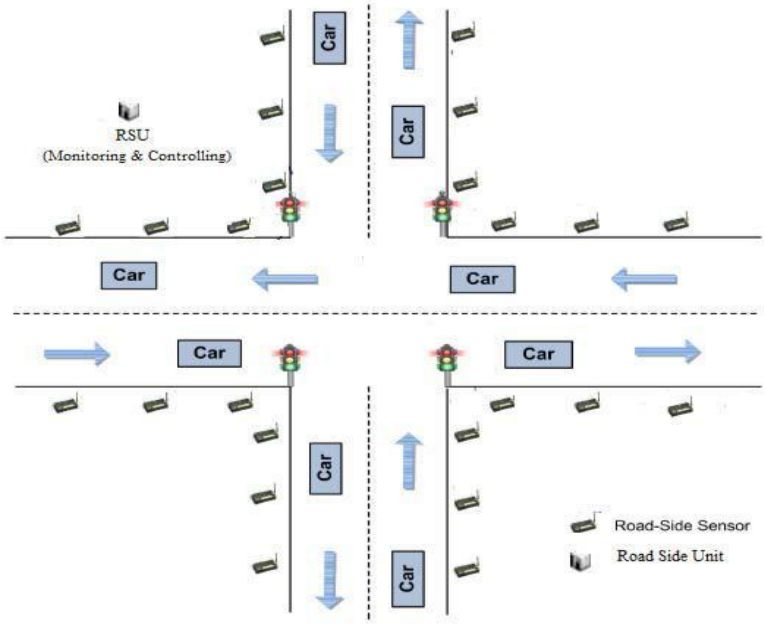

Рис. 3.1 Архітектура системи

У цьому розділі представлена робоча теорія системи моніторингу і управління транспортним засобом в режимі реального часу з використанням платформи IoT. У пропонованій системі є масив ультразвукових датчиків, обладнаних на узбіччі дороги для контролю рівня руху. Придорожні датчики виявляють транспортні засоби і знаходять рівень руху на цій смузі. Такі рівні є низькими, середніми і високими, які встановлюються на певній відстані. Дані сприймаються безперервно і посилаються в контролер для виявлення рівнів трафіку. Якщо рівень трафіку високий, то синхронізація

сигналу контролера, що управляє, на цій смузі і дає більше часу для проходження транспортних засобів. Якщо низький рівень трафіку виявляє, то синхронізація сигналу контролера, що управляє, в цій смузі дає менше часу для проходження транспортного засобу. Так що ця система віддає пріоритет аварійному автомобілю при високому рівні руху. Контролер взаємодіє з системою пріоритетів через радіочастотні приймачі. Він використовується для передачі, а також прийому застережливого повідомлення або будь-якого стану трафіку від блоку контролера до системи пріоритету. Ці ж дані відображаються у блоці рідкокристалічного дисплея (LCD). Інформація про рівні трафіку і його часу і дату, відправлена на сервер авторизованого відкритого початкового коду. Ці дані аналізуються за допомогою відкритого початкового коду аналітики Інтернету речей і зберігаються у базі даних сервера для подальшого аналізу. Блок-схема пропонованої системи показана на рис 3.2.

Блок-схема пропонованої системи показує інтеграцію ультразвукових датчиків з контролером ARM 7, який є вхідною стороною системи. ARM 7 також інтегрується з клавіатурою, радіочастотним приймачем, сигналом LED 'S, блоком LCD для виведення на дисплей, модулем Wi - Fi для передачі даних в Інтернет (сервер). Пропонована система розділена на дві основні частини: а) Апаратне б) Програмне забезпечення.

а) Апаратна частина системи складається з набору ультразвукових датчиків. (HC - SR04) для визначення рівня трафіку, ARM 7 контролер (LPC2138) для обробки даних, що перетворює аналогові в цифрові дані, мікроконтролер PIC, використовуваний для обробки даних, які приймаються блоком контролю і управління, клавіатура для вибору стану трафіку, 16 * 2 LCD для виходів дисплея, модуль Wi - Fi (ESP8266) для передачі даних в Інтернет (сервер) і радіочастотний приймач (CC2500) передає і приймає масаж або будь-який застережливий повідомлення, пов'язаний з трафік.

— Масив ультразвукових датчиків. Ультразвукові датчики - це не що інше, як ультразвукові перетворювачі, що перетворюють ультразвукові хвилі в електричні і навпаки. У цій роботі HC - SR04 ультразвукові датчики, використовувані для визначення рівнів руху транспортного засобу на перехресті, які відстежують дані про рух в режимі реального часу. Діапазон ультразвукового датчика для виявлення об'єкту складає від 2 см до 4 м і працює на частоті 40 кГц. Ці датчики легко розгортаються, мають високочастотну роботу і низьку вартість технічного обслуговування. Приймає і відображає дані від ультразвукових датчиків через контролер.

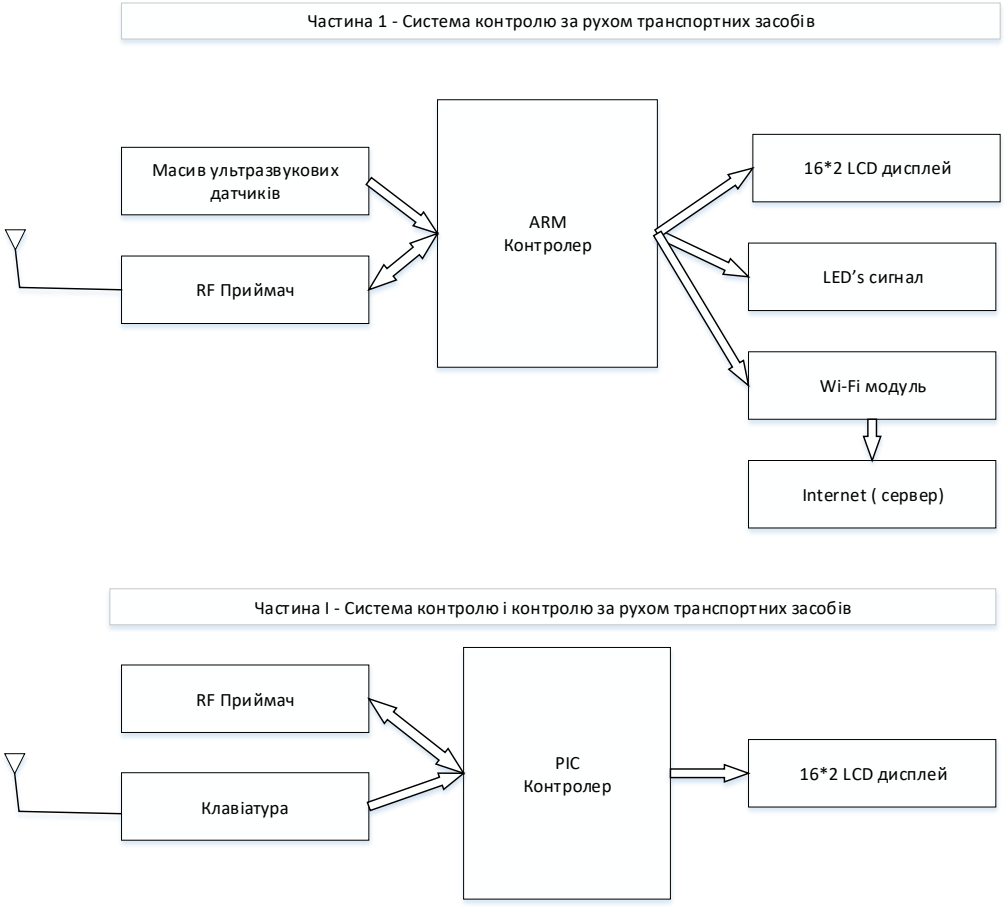

Рис 3. 2 Блок-схема пропонованої системи

— Контролер ARM 7 LPC2138 є високоефективним 32-бітовим мікро диспетчером RISC на ROM спалаху чіпа, RAM 32 КБ два 8 аналого-цифрових перетворювачів 10 бітів каналу, два послідовні інтерфейси I2C, годинник центрального процесора до 60 мГЦ, годинника реального часу з

додатковим резервним акумулятором, який корисний для цього застосування. Із-за низького енергоспоживання і малого розміру він використовувався в цій системі.

— Модуль Wi – Fi. ESP8266 модуль є набором високопродуктивних, високоінтегрованих безпровідних SOC. Він забезпечує можливість впровадження можливостей Wi - Fi в інших системах. Це автономне застосування, що має нижчу вартість і менше необхідного простору. Тут він використовується для передачі даних в режимі реального часу на сервер з боку контролера.

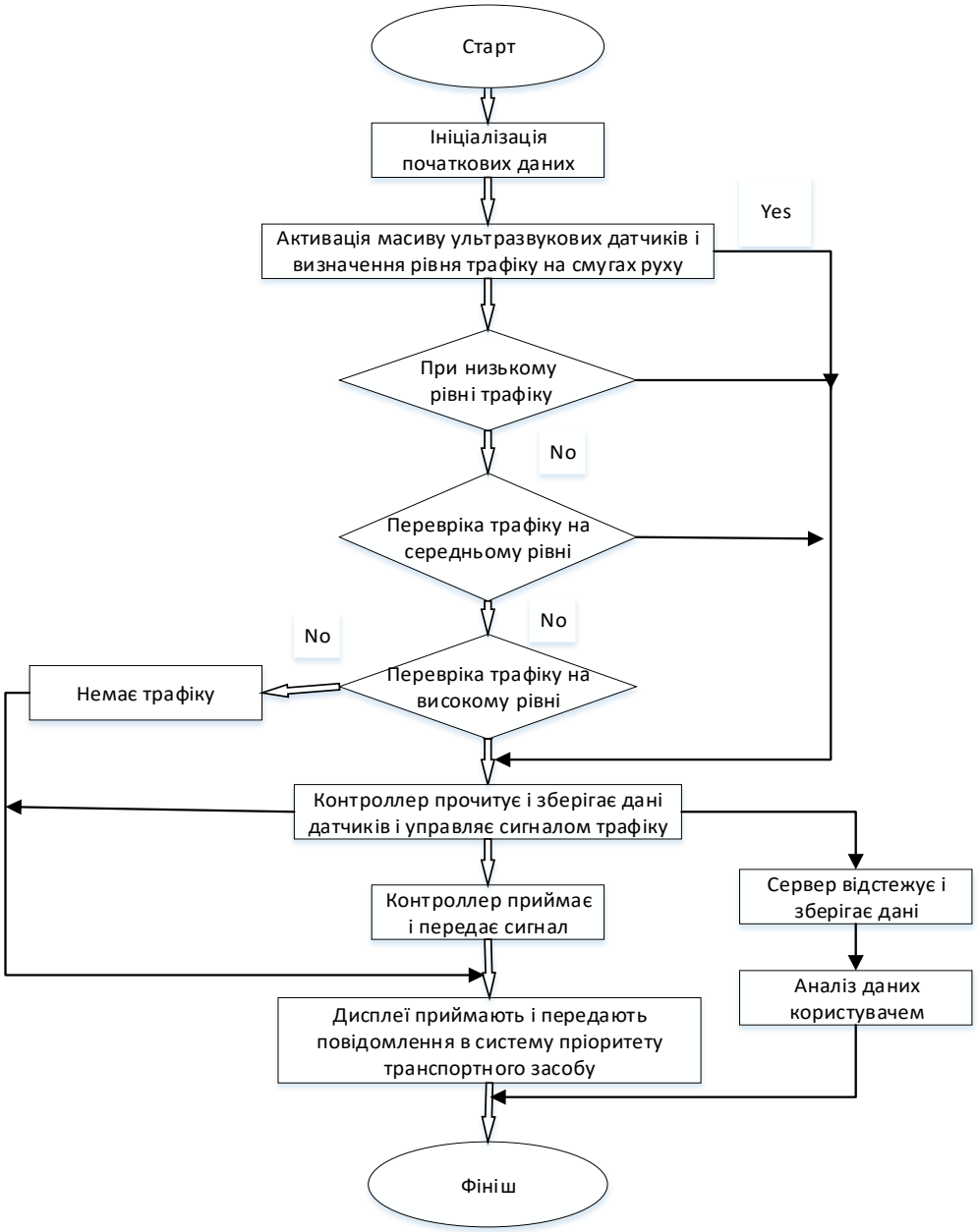

Рис. 3.3 Блок-схема експериментальних етапів

— Приймач РЧ приймач CC2500 це високошвидкісний модуль передачі даних, працюючий на частоті 2,4 ГГц. Тут він використовується для прийому, а також передачі даних від контролера. Цей модуль об'єднує схеми передавача і приймача.

— Мікродиспетчер PIC 18f4520 PIC є флеш-мікроконтролер, що має 10 розрядний аналого-цифровий перетворювач. Вона працює в діапазоні 40 кГц, забезпечує високу продуктивність, програмне забезпечення, низьку вартість і низьке енергоспоживання, тому використовується в системі пріоритету транспортного засобу.

— Сигнал LED’s. Цей блок використовувався тут для перетину доріг. Сигнали LED’s управляються алгоритмом управління сигналом трафіку, який видається за вимірювальними даними на рівнях від ультразвукових датчиків.

— LCD. Рідкокристалічний дисплей 16 * 2, використовуваний для спостереження за вихідними даними, заданими контролером. Він відображає рівні трафіку і час сигналу світлодіодам, а також повідомлення від РЧ приймача ЖК-дисплея, інтегрованого з мікроконтролером для відображення вихідних даних.

б) Програмне забезпечення. В цій роботі для аналізу використовується аналітика IoT з відкритим початковим кодом для даних трафіку в реальному часі. Він створює через користувача канали для побудови графіків в реальному часі з використанням доріжок для виявлення рівнів з використанням окремої IP-адреси. Після завантаження коду на сервер він відображає результати в реальному часі. Код написаний на мові C. Дані трафіку в реальному часі, завантажені на сервер, який передається з модуля Wi, - Fi, який приймається контролером. Сервер виконує наступні основні функції:

— Приймає і відображає дані від ультразвукових датчиків через контролер.

— Зберігає дані датчика у базі даних сервера для подальшого аналізу.

— Передає дані ультразвукового датчика кінцевому користувачеві для аналізу даних. В даному випадку система моніторингу і управління і пріоритетний системний код надаються на мові C, яка є надійною і легко зрозумілим для користувача. За допомогою Kiel програмний код записується в систему.

в) Блок-схема. Програмна реалізація цієї системи розроблена з використанням блок-схеми, показаної на рис 3.4.

г) Розробка системи Запропонована конструкція системи виконана в двох частинах, перша - блок контролю і управління транспортним засобом, а друга - блок пріоритету транспортного засобу. Перед реалізацією прототипу тестуються усі компоненти і пристрої. Прототипи реалізації цих двох частин показані на рис. 3.4 і рис. 3.5.

— Блок управління і контролю транспортного засобу. В цій частині контролер ARM взаємодіє з ультразвуковими датчиками, клавіатурою, модулем Wi - Fi, LCD дисплеєм, LEDs сигналом світлодіодів і RF радіочастотним приймачем, які показані на рис. 3.4.

— Пріоритетна частина транспортного засобу. В цій частині мікроконтролер PIC взаємодіє з RF приймачем, клавіатурою і LCD дисплеєм. Прототип реалізації цієї частини показаний на рис. 3.5.

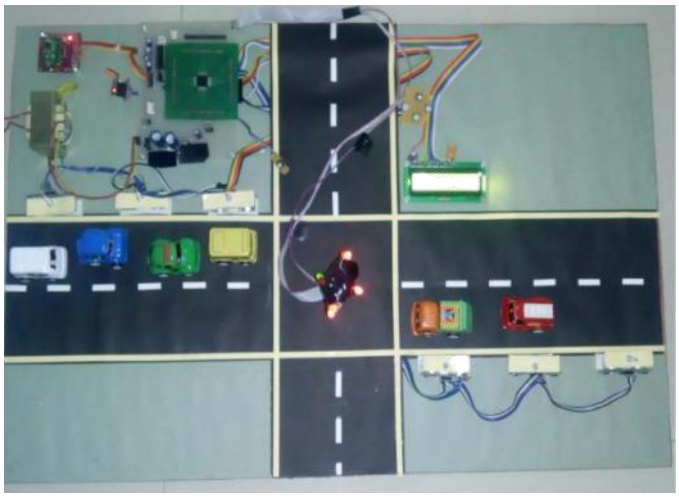

Рис 3.4 Експериментальна установка для контролю і управління рухом транспортного засобу

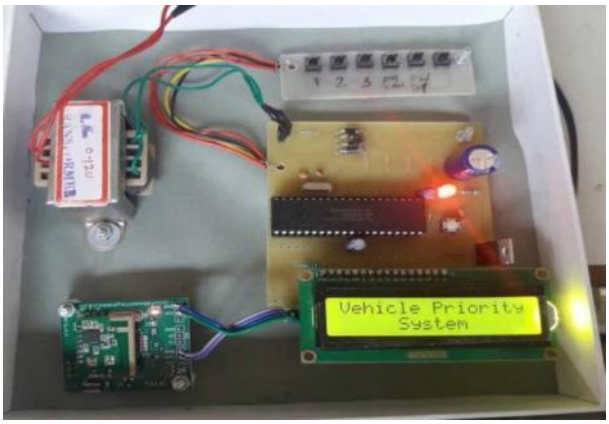

Рис 3.5 Експериментальна установка для пріоритетної частини транспортного засобу

3.3 Результати дослідження

Платформа IoT для системи моніторингу трафіку в режимі реального часу за допомогою ультразвукових датчиків виявляє рівні трафіку на маршрутах TR1 а TR2 показує на ЖК-дисплеї. На рис. 3.6 показані рівні трафіку транспортного засобу на маршрутах TR1 і TR2 і синхронізація сигналу відповідно до алгоритму управління сигналом трафіку. TR1 вказує на високий рівень трафіку, тому найвищий пріоритет віддається цій смузі, а TR2 вказує на середній рівень трафіку, так що він дає менше часу сигналу, чим TR1.

Рис. 3.6 Рівень трафіку на ЖК-дисплеї

На рис.3.6 показано повідомлення про вибір смуги руху системи пріоритету транспортного засобу, який відображається на ЖК-дисплеї. Це повідомлення передається в систему контролера через радіочастотний приймач.

Рис. 3.7 Вибір смуги руху за системою пріоритетів транспортного засобу

Результати експерименту видимі на сервері з будь-якого місця у світі, де використовуються IP-адреси. Результати отримані з графіків рівнів руху в реальному часі на смугах рухи, які показані на рис. 3.6 і рис.3.7.

Рис. 3.4. Рівень руху в першій смузі

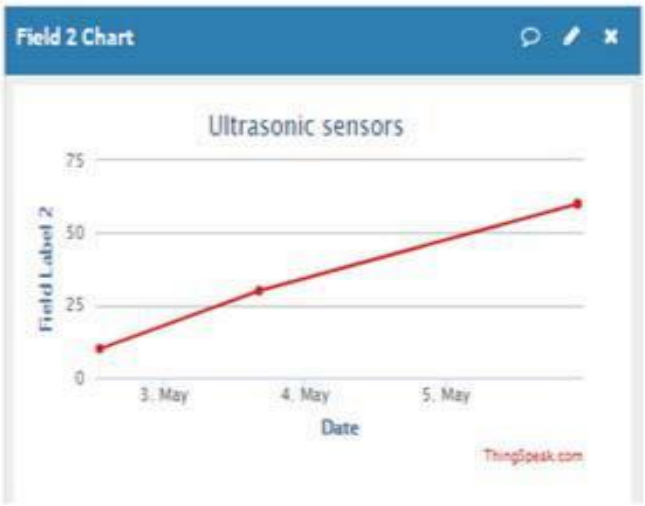

Рис. 3.5 Рівень руху на другій смузі

Висновки:

Наша країна займає найвище місце у світі по проблемах, пов'язаних з дорожнім рухом, тому є необхідність скоротити питання, пов'язані з дорожнім рухом, такі як тривалий час пересування, витрати палива, забруднення повітря і проблеми, пов'язані з транспортом була запропонована система. Тут представлена вдосконалена система моніторингу трафіку в режимі реального часу з використанням платформи IoT, яка є надійною для користувачів. Ця система також контролює час сигналу, відповідно до рівнів руху на смугах руху, віддає пріоритет аварійному автомобілю. Використовуючи систему моніторингу

транспортного засобу як типовий приклад, ми перевірили, що система досягла хорошої продуктивності в практичному сценарії застосування. Запропонована система є надійнішою, легко працює користувачами і недорогою системою і легко може бути встановлена у будь-якому місці.

Головна мета досягнута і система може надавати інформацію про датчики в реальному часі кінцевим користувачам. Реалізація даної системи зменшить навантаження на трафік на автошляхах і дозволить розумно користуватись та з користю, та особливо заощаджувати свій дорогоцінний час. Відмітимо, що для подальших досліджень як і раніше залишається багато цікавих напрямів.

ЗАГАЛЬНІ ВИСНОВКИ ПО РОБОТІ

В роботі було розглянуто основні терміни мережі Інтернет речей, досліджено архітектуру та основні компоненти IoT. Наведено характеристики всіх основних елементів. Було розглянуто безпеку і захисти безпеки IoT. Наведено переваги та недоліки, які притаманні мережам IoT. Після аналізу переваг та недоліків моделі IoT можна зробити висновок, що попри те, що переваг набагато більше ніж недоліків, на даний момент повноцінне використання Інтернет речей можливе з повними захистами безпеки та конфіденційності.

В роботі розглянуто моніторинг і основні платформи для моніторингу трафіку, які використовуються в більшості країн світу. Найпопулярнішими на сьогоднішній день являються платформи моніторингу трафіку ZABBIX, OpenView, Cacti. Були розглянуті такі спеціалізовані системи автоматизованого моніторингу дорожнього руху: OnStar, NEXCO Central, ECall Japan, ECall Europe. Також розглянуто такі системи як: система аналізу дорожнього руху (RTA), Моха та система моніторингу дорожнього руху в режимі реального часу з використанням алгоритму SAR**.** Таким чином, проаналізувавши всі системи моніторингу дорожнього руху було прийнято рішення, яке буде ефективнішим –це інтеграція розглянутих систем в одній універсальній та дозволяє забезпечити автомобіліста повним спектром послуг, починаючи від ефективної навігації закінчуючи цілодобовим наданням інформації про автотранспортний засіб. Проаналізувавши інтегровану систему, ціль якої спрямована як на моніторинг кожного автомобіля окремо, так і на контроль дорожнього руху в цілому та зменщення наванатжень на дорогах, а саме повний контроль впорядку пріоритетності всього трафіку, також потребувла удосконалення. Отож, система має надавати можливість автоматизувати процеси оптимального управління транспортними засобами і дорожнім рухом в режимі реального часу для вирішення соціальних, гуманітарних, економічних і екологічних проблем.

Була вдосконалена система моніторингу трафіку в режимі реального часу з використанням платформи IoT в режимі реального часу з використанням платформи IoT, яка є надійною для користувачів. Ця система також контролює час сигналу, відповідно до рівнів руху на смугах руху, віддає пріоритет аварійному автомобілю. Використовуючи систему моніторингу транспортного засобу як типовий приклад, ми перевірили, що система досягла хорошої продуктивності в практичному сценарії застосування. Запропонована система є надійнішою, легко працює користувачами і недорогою системою і легко може бути встановлена у будь-якому місці.

Головна мета досягнута і система може надавати інформацію про датчики в реальному часі кінцевим користувачам. Реалізація даної системи зменшить навантаження на трафік на автошляхах і дозволить розумно користуватись та з користю, та особливо заощаджувати свій дорогоцінний час. Відмітимо, що для подальших досліджень як і раніше залишається багато цікавих напрямів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Аналитика SAS для IoT // електрон. текст. дані URL: https://www.sas.com/ru_ua/software/analytics-iot.html (дата звернення: 01.05.2020)

2. Архітектура і технології IoT // електрон. текст. дані URL: https://learn.ztu.edu.ua/pluginfile.php/68838/mod_resource/content/2/%D0%9B-1.pdf (дата звернення: 01.05.2020)

3. Чотири етапи та архітектури Інтернету речей // електрон. текст. дані URL: https://medium.com/datadriveninvestor/4-stages-of-iot-architecture-explained-in-simple-words-b2ea8b4f777f (дата звернення: 03.05.2020)

4. The 4 stages of an IoT architecture // електрон. текст. дані URL: https://techbeacon.com/enterprise-it/4-stages-iot-architecture (дата звернення: 03.05.2020)

5. What is Internet of Things (IoT) and How it Works? // електрон. текст. дані URL: https://appinventiv.com/blog/what-is-internet-of-things/ (дата звернення: 03.05.2020)

6. The advantages and disadvantages of Internet Of Things // електрон. текст. дані URL: https://e27.co/advantages-disadvantages-internet-things-20160615/ (дата звернення: 03.05.2020)

7. Welcome on Star // електрон. текст. дані URL: https://www.onstar.com/ web/portal/termsconditions / (дата звернення: 12.05.2020)

8. Применение оборудования MOXA в дата-центрах // електрон. текст. дані URL: https://moxa.pro/articles/articles/primenenie-oborudovaniya-moxa-v-data-tsentrakh/ / (дата звернення: 15.05.2020)

9. Monitoring and Integration Solution // електрон. текст. дані URL: https://www.zabbix.com/integrations?cat=services// /(дата звернення: 16.05.2020)

10. IEEE 1451 Smart Transducer Interface Standards // електрон. текст. дані URL: www.nist.gov/el/isd/ieee/IEEE 1451.cfm (дата звернення:

18.05.2020)

11. Filjar. R. ECall: Automatic notification of a road traffic accident / K.Vidovic, P.Britvic, M. Rimac // MIPRO. 2011. C. 600-605.

12. Using GPS / TS Wey, MH Lin, NT Hu A// Display technology. 2011. C. 45-53.

13. Pinart Carolina. ECallcompliant early crash notification service for portable and nomadic devices / J. Carlos Calvo, Laura Nicholson, Jos A. Villaverde// MIT. 2011. C. 134-146.

14. Werner Marc. Cellular In-Band Modem Solution for eCall Emergency Data Transmission / Christian Pietsch, Christoph Joetten // Communication. 2009. C. 198-207.

15. Kohn Andreas. The eCall Program: Overview and Design Considerations // Sierra Wireless. 2010. P. 157-167p.

16. T. Sukuvaara, P. Nurmi, M. Hippi, R. Autio, D. Stepanova, P. Eloranta, L. Riihentupa and K. Kauvo / Wireless traffic safety network for incident and weather information, 1st ACM International Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications/ 4 November 2011

17. M. Kutila, P. Pyykönen, K. Kauvo, and P. Eloranta / In-vehicle sensor data fusion for road friction monitoring IEEE / 2011

18. M. Kutila, P. Pyykönen, J. Yliaho, and B. Rössler / Co-operative intersection infrastructure monitoring system Advanced Microsystems for Automotive Applications - AMAA 2010 / Berlin, Germany, 2010.

19. A. Whitmore, A. Agarwal, and L. Da Xu / The Internet of Things—A survey of topics and trends / C. 261-274, 2015.